SecurityScorecard

Scorecard for Fiserv

Generated February 1, 2019
by Dana Bowers (dana.bowers@venminder.com), Venminder

About this file

This file is a point-in-time capture of this Scorecard as of 2:14:15 PM EST, February 1, 2019.
This file should not be confused for a pen test result or a final assessment.

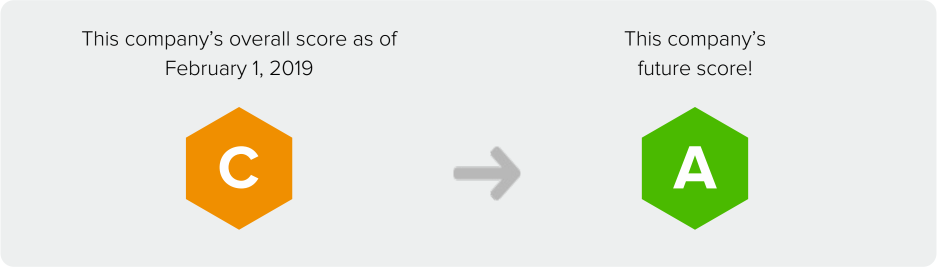
What is SecurityScorecard?

SecurityScorecard is a security ratings service that uses an easy-to-understand A-F grading system to rate companies on their overall security as well as across 10 major risk factors. A company with a C, D, or F rating is 5.4 times more likely to suffer a consequential breach versus A or B-rated companies[1]. Certain risk factors, such as application security and patching cadence, are even more indicative of the likelihood of breach. An F versus an A in these factors may translate into a tenfold increase in the likelihood of a data breach or successful attack.

Learn more about SecurityScorecard's rating system at bit.ly/2zMLSmW.

[1] 'New SecurityScorecard Research Can Help You Detect a Data Breach Before It Happens', bit.ly/2yc0JVN

Next Steps: Get to an A



This company's overall score as of February 1, 2019

This company's future score!

1. Create an account

This file has a lot of detail but remember, it's only for one point in time. Create an account to get full free access to your organizaton's Scorecard along with ongoing self-monitoring, history reports, CSV data exports and more.

2. Validate your Digital Footprint

Once you have an account, review your company's Digital Footprint, the assets SecurityScorecard found as potentially attributable to your company that affect the ratings in your Scorecard. Request removal or addition of IPs as needed.

3. Review issue findings

Investigate the contents of your Scorecard with your team(s). It's a win for your company's security posture when you identify loose ends of which you weren't aware.

4. Remediate issues, improve your score

Whether you've deployed a fix, found assets that don't belong to your company, or want to share information about compensating controls, you can let us know by remediating the identified finding(s) and submitting them for resolution approval. Resolutions are handled by our Support team, which will resolve any outstanding item within three business days. Remediate issues within the platform or email support@securityscorecard.io.

We're here to help

The SecurityScorecard platform is based on transparency and collaboration. Our Customer Reliability Support team provides remediation and resolution services at no charge and are happy to work with you and your customers to resolve any issues. If you need assistance at any stage, get in touch by emailing support@securityscorecard.io.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Scorecard Overview

C

Fiserv

76 Security Score

DOMAIN: fiserv.com

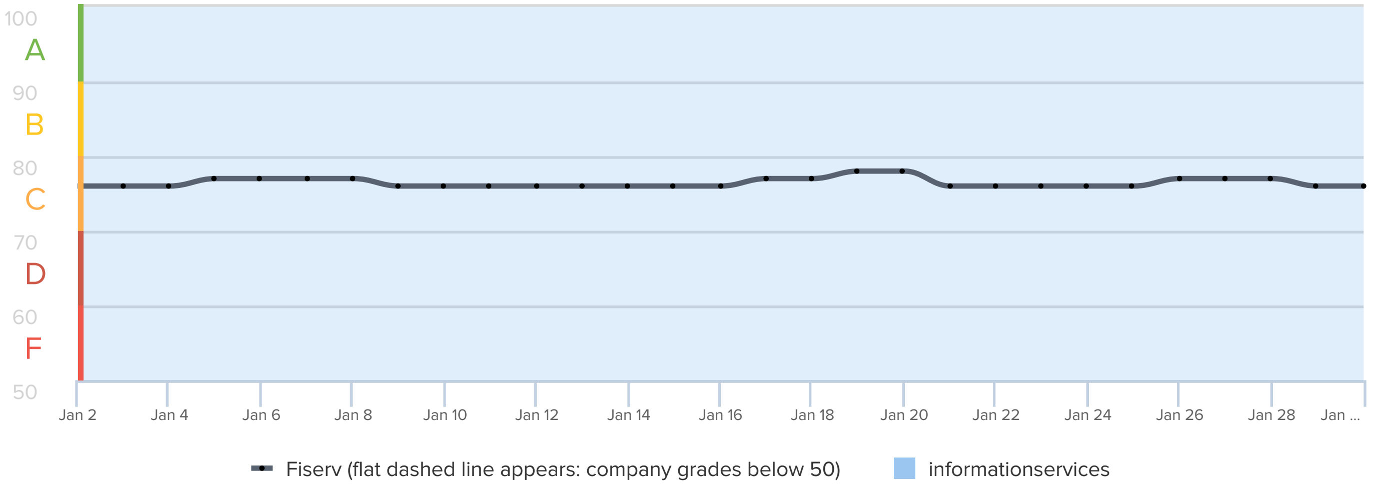
INDUSTRY: INFORMATION SERVICES

Factors

C	73	NETWORK SECURITY	20 ISSUES
F	51	DNS HEALTH	3 ISSUES
C	76	PATCHING CADENCE	6 ISSUES
B	89	ENDPOINT SECURITY	1 ISSUE
A	100	IP REPUTATION	1 ISSUE
F	58	APPLICATION SECURITY	13 ISSUES
C	70	CUBIT SCORE	1 ISSUE
A	100	HACKER CHATTER	0 ISSUES
A	100	INFORMATION LEAK	0 ISSUES
A	100	SOCIAL ENGINEERING	1 ISSUE

30-Day Score History

The chart below shows the evolution of the company's relative security ranking over time. The shaded area represents the range of values taken by companies in the INFORMATION SERVICES industry.



Peaks in score performance represent improvements to overall security posture, remediation of open issues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Action Items

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
IP Reputation	!	N/A	Malware Events, Last Year. Communications indicative of malware infections were observed over the last 365 days.
Endpoint Security	!!	-0.4	Outdated Web Browser Observed. An outdated web browser connected to a web server.
Patching Cadence	!!!	-0.4	High-Severity Vulnerability in Last Observation. We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.
	!!!	-0.9	High Severity CVEs Patching Cadence. High severity vulnerability seen on network more than 30 days after CVE was published.
	!!	-0.4	End-of-Life Product. We observed an end-of-life product, one that is no longer developed or sold, publicly exposed.
	!!	-0.6	Medium-Severity Vulnerability in Last Observation. We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.
	!!	-0.7	Medium Severity CVEs Patching Cadence. Medium severity vulnerability seen on network more than 60 days after CVE was published.
	!!	-0.1	End-of-Service Product. We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed.
Network Security	!!!	-0.5	SSH Software Supports Vulnerable Protocol. Server(s) observed running SSH software that support an SSH protocol lower than version 2.
	!!	-0.2	MySQL Service Observed. We observed MySQL, a database management system, publicly exposed.
	!!	-0.7	SSL Certificate Uses Weak Signature. TLS analysis reveals a weak signature algorithms, using SHA1 or MD5.
	!!	-0.3	SSH Supports Weak MAC. A weak Message Authentication Code (MAC) algorithm has been detected.
	!!	-0.3	SSH Supports Weak Cipher. A weak cipher has been detected.
	!!	-0.1	Microsoft SQL Server Service Observed. We observed Microsoft SQL Server, a database management system, publicly exposed.
	!!	-0.2	Certificate Is Self-Signed. Servers presenting self-signed certificates trigger warnings in, or prevent connections from TLS clients.
	!!	-0.6	Certificate Is Expired. Expired certificates prevent TLS clients from connecting to servers.
	!!	-<0.1	IMAP Service Observed. We observed IMAP, an email retrieval service, publicly exposed.
	!!	-0.1	RDP Service Observed. We observed RDP, a remote access service, publicly exposed.
	!!	-0.5	TLS Protocol Uses Weak Cipher. TLS analysis reveals a weak cipher either through encryption protocol or public key length.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	!!	-0.2	SMB Service Observed. We observed SMB, a file and printer-sharing service, publicly exposed.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
Network Security	!	-<0.1	TLS Certificate Without Revocation Control. We observed a TLS certificate that did not contain either CRL or OCSP URLs.
	!	-0.1	FTP Service Observed. We observed FTP, a file-sharing service, publicly exposed.
	!	-<0.1	Telnet Service Observed. We observed Telnet, a remote access service, publicly exposed.
	!	-0.1	Certificate Lifetime Is Longer Than Best Practices. We observed a certificate with a lifetime longer than 39 Months.
Cubit Score	!	-1.0	Exposed Subdomain. An administrative subdomain was detected on public Internet. That subdomain may be vulnerable to unauthorized access.
Application Security	!!!	-1.6	Site does not enforce HTTPS. Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code).
	!!	-0.9	Website does not implement X-Frame-Options Best Practices. Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks.
	!!	-1.0	Website Does Not Implement HSTS Best Practices. Even if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website.
	!!	-0.9	Website does not implement X-XSS-Protection Best Practices. Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks.
	!!	-0.9	Redirect Chain Contains HTTP. Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site.
	!!	-0.9	Insecure HTTPS Redirect Pattern. Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site.
	!	-0.2	Session Cookie Missing 'HttpOnly' Attribute. Data may be exposed to unauthorized parties during cookie transmission and increases the risk of cross-site scripting (XSS) attacks.
	!	-0.3	Website does not implement X-Content-Type-Options Best Practices. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript.
DNS Health	!!!	-2.4	Open DNS Resolver Detected. Misconfigured DNS services were detected

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DNS Health	!!!	-2.1	Open DNS Resolver Detected. Misconfigured DNS services were detected.
	!!	-4.3	SPF Record Missing. A missing SPF record has been detected for a domain.
	!	-1.6	SPF Record Contains a Softfail. Softfail attributes in SPF makes spoofing and phishing email possible.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

C 73 NETWORK SECURITY

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The Network Security module checks public datasets for evidence of high risk or insecure open ports within the company network. Insecure ports can often be exploited to allow an attacker to circumvent the login process or obtain elevated access to the system. If misconfigured, the open port can act as the entry point between a hacker's workstation and your internal network.

!!! HIGH SEVERITY	
SSH Software Supports Vulnerable Protocol	6
MongoDB Service Observed	0
Unauthenticated Elasticsearch Service Observed	0
Certificate Is Revoked	0

!! MEDIUM SEVERITY	
SSL Certificate Uses Weak Signature	24
TLS Protocol Uses Weak Cipher	33
Certificate Is Expired	81
Certificate Is Self-Signed	2
SSH Supports Weak Cipher	367
SSH Supports Weak MAC	96
SMB Service Observed	4
RDP Service Observed	1
MySQL Service Observed	1
Microsoft SQL Server Service Observed	1
IMAP Service Observed	1
Apache Cassandra Service Observed	0
Apache CouchDB Service Observed	0
PostgreSQL Service Observed	0
Redis Service Observed	0
rsync Service Observed	0
VNC Service Observed	0

! LOW SEVERITY	
Certificate Lifetime Is Longer Than Best Practices	6
Telnet Service Observed	3
FTP Service Observed	51
TLS Certificate Without Revocation Control	5

✓ POSITIVE SIGNALS	
TLS Certificate Status Request ("OCSP Stapling") Detected	163
Extended Validation Certificate Observed	17
DDoS Protection Service Detected	0

i INFORMATIONAL	
POP3 Service Observed	2
Open TCP Ports Observed	6

NETWORK SECURITY > ISSUE DETAIL

!!! SSH Software Supports Vulnerable Protocol

Server(s) observed running SSH software that support an SSH protocol lower than version 2.

-0.5 SCORE IMPACT

6 findings

BANNER	EVIDENCE	DESTINATION IP	DESTINATION PORT	LAST SEEN
SSH-1.99-Cisco-1.25\n	protocol 1.99	12.111.185.3	22	2019-01-09T18:35:31.265Z
SSH-1.99-Cisco-1.25\n	protocol 1.99	8.18.18.224	22	2019-01-09T15:40:05.164Z
SSH-1.99-Cisco-1.25\n	protocol 1.99	12.34.24.25	22	2019-01-09T14:54:13.389Z
SSH-1.99-Cisco-1.25\n	protocol 1.99	12.111.185.1	22	2019-01-09T09:03:31.584Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-1.99-Cisco-1.25\n	protocol 1.99	8.18.18.242	22	2019-01-09T07:25:19.459Z
-	protocol 1.99	12.111.185.2	22	2019-01-08T02:27:03.000Z

RECOMMENDATION

Configure the SSH service to support only SSH protocol version 2 or higher. Upgrade the SSH service software to the latest version of software.

ABOUT THIS ISSUE

Secure Shell (SSH) is an encrypted network protocol to allow remote login and other network services to operate securely over an unsecured network by providing an authenticated and encrypted channel. All modern SSH clients and servers support the more secure SSH protocol version 2, and any version older is exploitable and obsolete. Version 1 of the SSH protocol contains fundamental weaknesses including a design flaw that allows a man-in-the-middle attack. Findings are removed automatically if they have not been observed for more than 30 days.

NETWORK SECURITY > ISSUE DETAIL

SSH Supports Weak Cipher

A weak cipher has been detected.

-0.3 SCORE IMPACT

367 findings

BANNER	EVIDENCE	DESTINATION IP	DESTINATION PORT	LAST SEEN
SSH-2.0-Serv-U_15.1.4.6	rijndael-cbc@lysator.liu.se	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	blowfish-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	rijndael256-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	aes192-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	cast128-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	aes256-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-Serv-U_15.1.4.6	rijndael192-cbc	12.175.11.84	22	2019-01-09T21:06:31.168Z
SSH-2.0-9.99	cast128-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	3des-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	twofish-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	aes128-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	twofish128-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	blowfish-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	twofish256-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	aes256-cbc	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	arcfour	63.167.86.240	22	2019-01-09T20:44:40.680Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-9.99	blowfish-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	aes128-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	cast128-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	twofish-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	arcfour	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	aes256-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	3des-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	twofish256-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	twofish128-cbc	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	twofish-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	blowfish-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	aes128-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	cast128-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	twofish256-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	arcfour	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	3des-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	twofish128-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	aes256-cbc	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	twofish-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-9.99	aes128-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-9.99	twofish256-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-9.99	aes256-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-9.99	twofish128-cbc	192.131.55.3	22	2019-01-09T20:02:54.001Z
SSH-2.0-OBS	arcfour128	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	aes192-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	aes256-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	aes128-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	3des-cbc	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	arcfour256	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	aes256-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	arcfour128	198.167.0.223	22	2019-01-09T19:46:51.225Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-OBS	3des-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	aes192-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	arcfour256	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	aes128-cbc	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-1.82_sshlib	3des-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	blowfish-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	aes128-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	twofish-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	aes256-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	twofish256-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	cast128-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	arcfour	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	twofish128-cbc	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-OBS	aes128-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	aes256-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	3des-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	aes192-cbc	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-VShell_4_2_3_1188	twofish-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-VShell_4_2_3_1188	3des-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-VShell_4_2_3_1188	aes256-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-VShell_4_2_3_1188	blowfish-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-VShell_4_2_3_1188	aes192-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-VShell_4_2_3_1188	aes128-cbc	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-VShell_4_2_3_1188	arcfour	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-OBS	arcfour256	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	3des-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-OBS	blowfish-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	aes128-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	aes192-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	aes256-cbc	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	arcfour128	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OpenSSH_5.4p1	aes256-cbc	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-OpenSSH_5.4p1	aes128-cbc	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-OpenSSH_5.4p1	arcfour	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-OpenSSH_5.4p1	arcfour256	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-9.99	twofish128-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	aes256-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	twofish-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	3des-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	cast128-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	blowfish-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	arcfour	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	aes128-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	twofish256-cbc	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-OBS	arcfour256	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	aes128-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	3des-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	aes192-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	aes256-cbc	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	arcfour128	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	arcfour256	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	3des-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	aes192-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	aes128-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	aes256-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	arcfour128	198.167.0.172	22	2019-01-09T18:42:05.949Z

SSH-1.99-Cisco-1.25	aes256-cbc	12.111.185.3	22	2019-01-09T18:35:31.137Z
SSH-1.99-Cisco-1.25	3des-cbc	12.111.185.3	22	2019-01-09T18:35:31.137Z
SSH-1.99-Cisco-1.25	aes192-cbc	12.111.185.3	22	2019-01-09T18:35:31.137Z
SSH-1.99-Cisco-1.25	aes128-cbc	12.111.185.3	22	2019-01-09T18:35:31.137Z
SSH-2.0-OBS	arcfour128	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	arcfour256	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	aes128-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	aes192-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	aes256-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	3des-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	3des-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	arcfour256	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	aes128-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	aes256-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	aes192-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	arcfour128	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-Cisco-1.25	aes192-cbc	65.202.81.137	22	2019-01-09T18:23:57.424Z
SSH-2.0-Cisco-1.25	aes128-cbc	65.202.81.137	22	2019-01-09T18:23:57.424Z
SSH-2.0-Cisco-1.25	aes256-cbc	65.202.81.137	22	2019-01-09T18:23:57.424Z
SSH-2.0-Cisco-1.25	3des-cbc	65.202.81.137	22	2019-01-09T18:23:57.424Z
SSH-2.0-9.99	twofish-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	arcfour	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	blowfish-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	cast128-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	twofish128-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	aes256-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	twofish256-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	3des-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	aes128-cbc	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-Cisco-1.25	aes192-cbc	12.2.10.241	22	2019-01-09T17:20:56.565Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-Cisco-1.25	3des-cbc	12.2.10.241	22	2019-01-09T17:20:56.565Z
SSH-2.0-Cisco-1.25	aes128-cbc	12.2.10.241	22	2019-01-09T17:20:56.565Z
SSH-2.0-Cisco-1.25	aes256-cbc	12.2.10.241	22	2019-01-09T17:20:56.565Z
SSH-2.0-OBS	aes128-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	arcfour128	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	aes192-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	arcfour256	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	3des-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	aes256-cbc	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-9.99	twofish128-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	aes128-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	cast128-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	twofish256-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	3des-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	aes256-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	twofish-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	arcfour	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-9.99	blowfish-cbc	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-1.82_sshlib	twofish256-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	cast128-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	aes256-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	aes128-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	arcfour	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	3des-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	twofish-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	twofish128-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	blowfish-cbc	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-9.99	aes128-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	arcfour	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	twofish-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-9.99	twofish128-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	3des-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	blowfish-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	twofish256-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	cast128-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	aes256-cbc	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-1.99-Cisco-1.25	aes256-cbc	12.34.24.25	22	2019-01-09T14:54:14.588Z
SSH-1.99-Cisco-1.25	aes128-cbc	12.34.24.25	22	2019-01-09T14:54:14.588Z
SSH-1.99-Cisco-1.25	aes192-cbc	12.34.24.25	22	2019-01-09T14:54:14.588Z
SSH-1.99-Cisco-1.25	3des-cbc	12.34.24.25	22	2019-01-09T14:54:14.588Z
SSH-2.0-OBS	aes256-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	arcfour256	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	3des-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	aes192-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	aes128-cbc	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	arcfour128	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-9.99	aes256-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	blowfish-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	arcfour	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	cast128-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	twofish128-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	aes128-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	3des-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	twofish256-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	twofish-cbc	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-OBS	arcfour128	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	aes256-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	aes128-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	arcfour256	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	aes192-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-OBS	3des-cbc	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	arcfour256	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	arcfour128	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	aes128-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	aes256-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	aes192-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	3des-cbc	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	arcfour256	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	aes192-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	arcfour128	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	aes128-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	aes256-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	3des-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	aes256-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	3des-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	arcfour256	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	aes192-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	aes128-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	arcfour128	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-9.99	aes128-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	twofish256-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	3des-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	cast128-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	twofish-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	aes256-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	blowfish-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	twofish128-cbc	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	arcfour	65.213.167.80	22	2019-01-09T12:41:55.960Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-OBS	aes192-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	aes128-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	3des-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	aes256-cbc	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	arcfour256	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	arcfour128	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-mod_sftp/0.9.9	arcfour128	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	aes256-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	3des-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	blowfish-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	arcfour256	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	aes192-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	cast128-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	aes128-cbc	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-9.99	twofish-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	3des-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	twofish256-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	blowfish-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	aes128-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	cast128-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	twofish128-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	aes256-cbc	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	blowfish-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	aes256-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	twofish128-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	twofish-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	cast128-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	arcfour	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	twofish256-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	3des-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-9.99	aes128-cbc	63.167.86.246	22	2019-01-09T11:35:22.579Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-dropbear_2014.65	twofish-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0-dropbear_2014.65	twofish128-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0-dropbear_2014.65	aes128-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0-dropbear_2014.65	aes256-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0-dropbear_2014.65	3des-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0-dropbear_2014.65	twofish256-cbc	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0-VShell_3_6_6_741	aes256-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-VShell_3_6_6_741	arcfour	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-VShell_3_6_6_741	aes192-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-VShell_3_6_6_741	3des-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-VShell_3_6_6_741	blowfish-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-VShell_3_6_6_741	twofish-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-VShell_3_6_6_741	aes128-cbc	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-OBS	arcfour128	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	arcfour256	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	aes256-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	aes192-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	aes128-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	3des-cbc	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	arcfour128	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	3des-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	aes128-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	aes192-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	aes256-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-OBS	blowfish-cbc	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	arcfour256	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-9.99	twofish128-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	aes256-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	blowfish-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	cast128-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	arcfour	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	twofish256-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	3des-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	twofish-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	aes128-cbc	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-OBS	arcfour128	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	aes192-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	aes256-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	3des-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	arcfour256	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	aes128-cbc	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-5.37	3des-cbc	198.246.218.142	22	2019-01-09T09:22:42.918Z
SSH-2.0-5.37	aes256-cbc	198.246.218.142	22	2019-01-09T09:22:42.918Z
SSH-2.0-9.99	aes128-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	twofish-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	arcfour	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	twofish256-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	twofish128-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	aes256-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	cast128-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	3des-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	blowfish-cbc	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-OBS	3des-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	aes256-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	aes128-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-OBS	arcfour128	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	arcfour256	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	blowfish-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	aes192-cbc	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-9.99	cast128-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	arcfour	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	aes128-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	aes256-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	twofish128-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	3des-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	blowfish-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	twofish-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	twofish256-cbc	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	3des-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	twofish-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	aes128-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	arcfour	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	twofish256-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	cast128-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	twofish128-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	aes256-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	blowfish-cbc	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-1.99-Cisco-1.25	aes192-cbc	12.111.185.1	22	2019-01-09T09:03:31.581Z
SSH-1.99-Cisco-1.25	3des-cbc	12.111.185.1	22	2019-01-09T09:03:31.581Z
SSH-1.99-Cisco-1.25	aes256-cbc	12.111.185.1	22	2019-01-09T09:03:31.581Z
SSH-1.99-Cisco-1.25	aes128-cbc	12.111.185.1	22	2019-01-09T09:03:31.581Z
SSH-2.0-9.99	aes256-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	arcfour	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	twofish-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	3des-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	twofish128-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	aes128-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-9.99	cast128-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	twofish256-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	blowfish-cbc	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-OBS	arcfour256	198.167.0.142	22	2019-01-09T07:46:04.881Z
SSH-2.0-OBS	arcfour128	198.167.0.142	22	2019-01-09T07:46:04.881Z
SSH-2.0-VShell_3_8_2_229	aes128-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0-VShell_3_8_2_229	aes256-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0-VShell_3_8_2_229	arcfour	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0-VShell_3_8_2_229	blowfish-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0-VShell_3_8_2_229	3des-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0-VShell_3_8_2_229	aes192-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0-VShell_3_8_2_229	twofish-cbc	65.118.57.177	22	2019-01-09T07:29:18.485Z

RECOMMENDATION

Configure the SSH server to disable Arcfour and CBC ciphers.

ABOUT THIS ISSUE

The SSH server is configured to support either Arcfour or Cipher Block Chaining (CBC) mode cipher algorithms. SSH can be configured to use Counter (CTR) mode encryption instead of CBC. The use of Arcfour algorithms should be disabled.

NETWORK SECURITY > ISSUE DETAIL

SSH Supports Weak MAC

A weak Message Authentication Code (MAC) algorithm has been detected.

-0.3 SCORE IMPACT

96 findings

BANNER	EVIDENCE	DESTINATION IP	DESTINATION PORT	LAST SEEN
SSH-2.0-9.99	hmac-md5-96	208.66.22.159	22	2019-01-09T21:00:22.868Z
SSH-2.0-9.99	hmac-md5	208.66.22.159	22	2019-01-09T21:00:22.868Z
SSH-2.0-9.99	hmac-md5-96	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	hmac-md5	63.167.86.240	22	2019-01-09T20:44:40.680Z
SSH-2.0-9.99	hmac-md5	209.163.213.146	22	2019-01-09T20:30:04.493Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-9.99	hmac-md5-96	209.163.213.146	22	2019-01-09T20:30:04.493Z
SSH-2.0-9.99	hmac-md5	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	hmac-md5-96	192.131.55.67	22	2019-01-09T20:07:26.104Z
SSH-2.0-9.99	hmac-md5	208.66.22.64	22	2019-01-09T20:01:46.446Z
SSH-2.0-9.99	hmac-md5-96	208.66.22.64	22	2019-01-09T20:01:46.446Z
SSH-2.0-OBS	hmac-md5	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.131	22	2019-01-09T19:47:10.364Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-OBS	hmac-md5	198.167.0.223	22	2019-01-09T19:46:51.225Z
SSH-2.0-1.82_sshlib	hmac-md5-96	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-1.82_sshlib	hmac-md5	216.138.118.39	22	2019-01-09T19:46:10.417Z
SSH-2.0-OBS	hmac-md5	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.10	22	2019-01-09T19:37:04.641Z
SSH-2.0-VShell_4_2_3_1188	hmac-md5	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-VShell_4_2_3_1188	hmac-md5-96	50.58.8.116	22	2019-01-09T19:03:35.365Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OBS	hmac-md5	198.167.0.64	22	2019-01-09T18:53:53.441Z
SSH-2.0-OpenSSH_5.4p1	hmac-md5-96	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-OpenSSH_5.4p1	hmac-md5	65.206.30.70	22	2019-01-09T18:52:23.505Z
SSH-2.0-9.99	hmac-md5-96	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-9.99	hmac-md5	198.246.218.170	22	2019-01-09T18:50:59.851Z
SSH-2.0-OBS	hmac-md5	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.176	22	2019-01-09T18:46:08.827Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	hmac-md5	198.167.0.172	22	2019-01-09T18:42:05.949Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	hmac-md5	198.167.0.65	22	2019-01-09T18:34:38.454Z
SSH-2.0-OBS	hmac-md5	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.72	22	2019-01-09T18:26:37.652Z
SSH-2.0-9.99	hmac-md5	12.168.16.253	22	2019-01-09T18:16:32.721Z
SSH-2.0-9.99	hmac-md5-96	12.168.16.253	22	2019-01-09T18:16:32.721Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

SSH-2.0-OBS	hmac-md5-96	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-OBS	hmac-md5	198.167.0.67	22	2019-01-09T16:53:52.995Z
SSH-2.0-9.99	hmac-md5-96	12.179.188.12	22	2019-01-09T16:42:15.691Z
SSH-2.0-1.82_sshlib	hmac-md5-96	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-1.82_sshlib	hmac-md5	216.138.118.41	22	2019-01-09T16:05:05.408Z
SSH-2.0-9.99	hmac-md5-96	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	hmac-md5	65.213.167.45	22	2019-01-09T15:10:18.326Z
SSH-2.0-9.99	hmac-md5	208.66.22.71	22	2019-01-09T15:04:27.380Z
SSH-2.0-9.99	hmac-md5-96	208.66.22.71	22	2019-01-09T15:04:27.380Z
SSH-2.0-OBS	hmac-md5	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.179	22	2019-01-09T14:17:47.779Z
SSH-2.0-9.99	hmac-md5	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-9.99	hmac-md5-96	12.168.16.243	22	2019-01-09T14:11:21.447Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	hmac-md5	198.167.0.70	22	2019-01-09T13:45:18.353Z
SSH-2.0-OBS	hmac-md5	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.167	22	2019-01-09T13:39:55.641Z
SSH-2.0-OBS	hmac-md5	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.222	22	2019-01-09T13:29:09.742Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-OBS	hmac-md5	198.167.0.63	22	2019-01-09T13:28:03.599Z
SSH-2.0-9.99	hmac-md5	208.66.22.12	22	2019-01-09T12:50:38.795Z
SSH-2.0-9.99	hmac-md5-96	208.66.22.12	22	2019-01-09T12:50:38.795Z
SSH-2.0-9.99	hmac-md5-96	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-9.99	hmac-md5	65.213.167.80	22	2019-01-09T12:41:55.960Z
SSH-2.0-OBS	hmac-md5	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.61	22	2019-01-09T12:25:34.112Z
SSH-2.0-mod_sftp/0.9.9	hmac-md5-96	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-mod_sftp/0.9.9	hmac-md5	166.73.14.38	22	2019-01-09T11:47:29.765Z
SSH-2.0-9.99	hmac-md5-96	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	hmac-md5	12.168.17.243	22	2019-01-09T11:37:52.542Z
SSH-2.0-9.99	hmac-md5	63.167.86.246	22	2019-01-09T11:35:22.579Z

SSH-2.0-9.99	hmac-md5-96	63.167.86.246	22	2019-01-09T11:35:22.579Z
SSH-2.0-dropbear_2014.65	hmac-md5	65.206.30.72	22	2019-01-09T11:33:22.217Z
SSH-2.0-VShell_3_6_6_741	hmac-md5	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-VShell_3_6_6_741	hmac-md5-96	50.58.8.117	22	2019-01-09T11:12:04.590Z
SSH-2.0-OBS	hmac-md5	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.161	22	2019-01-09T11:03:03.327Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-OBS	hmac-md5	198.167.0.113	22	2019-01-09T10:58:56.163Z
SSH-2.0-9.99	hmac-md5-96	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-9.99	hmac-md5	69.51.33.93	22	2019-01-09T10:35:10.039Z
SSH-2.0-OBS	hmac-md5	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.170	22	2019-01-09T10:18:23.897Z
SSH-2.0-9.99	hmac-md5	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-9.99	hmac-md5-96	69.51.33.92	22	2019-01-09T09:21:09.251Z
SSH-2.0-OBS	hmac-md5	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-OBS	hmac-md5-96	198.167.0.180	22	2019-01-09T09:10:22.455Z
SSH-2.0-9.99	hmac-md5	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	hmac-md5-96	192.131.55.66	22	2019-01-09T09:03:55.169Z
SSH-2.0-9.99	hmac-md5-96	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	hmac-md5	69.9.254.12	22	2019-01-09T09:03:42.540Z
SSH-2.0-9.99	hmac-md5-96	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	hmac-md5	63.84.245.78	22	2019-01-09T08:05:53.337Z
SSH-2.0-9.99	hmac-md5-96	208.66.22.35	22	2019-01-09T07:50:09.004Z
SSH-2.0-9.99	hmac-md5	208.66.22.35	22	2019-01-09T07:50:09.004Z
SSH-2.0-9.99	hmac-md5-96	12.168.17.253	22	2019-01-09T07:34:44.151Z
SSH-2.0-9.99	hmac-md5	12.168.17.253	22	2019-01-09T07:34:44.151Z
SSH-2.0-VShell_3_8_2_229	hmac-md5	65.118.57.177	22	2019-01-09T07:29:18.485Z
SSH-2.0-VShell_3_8_2_229	hmac-md5-96	65.118.57.177	22	2019-01-09T07:29:18.485Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

RECOMMENDATION

Configure the SSH server to disable the use of MD5.

ABOUT THIS ISSUE

The SSH server is configured to support MD5 algorithm. The cryptographic strength depends upon the size of the key and algorithm that is used. A Modern MAC algorithms such as SHA1 or SHA2 should be used instead.

NETWORK SECURITY > ISSUE DETAIL

IMAP Service Observed

We observed IMAP, an email retrieval service, publicly exposed.

-<0.1 SCORE IMPACT

1 finding

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
Dovecot imapd	-	209.221.136.222	143	2018-12-30T14:58:32.606Z

Banner:
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.\r\n

RECOMMENDATION

Review the business necessity of hosting a public IMAP server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The IMAP protocol offers access to messages stored on email servers. IMAP servers frequently contain all messages ever sent or received by an email account, not just recent messages. We observed an IMAP service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or access the messages within. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

Microsoft SQL Server Service Observed

We observed Microsoft SQL Server, a database management system, publicly exposed.

-0.1 SCORE IMPACT

1 finding

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Microsoft SQL Server 2014	12.00.2269	184.170.226.96	1433	2019-01-21T12:50:15.000Z

RECOMMENDATION

Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

Microsoft SQL Server is a proprietary database management system (DBMS). DBMSes are intended to store large amounts of information. We observed a Microsoft SQL Server service on the Internet, accessible by the public. DBMSes are attractive targets to attackers due to the data they may contain. An attacker that breaches a DBMS may sell the databases within, use them for blackmail, or employ the information when launching further attacks. A breached database may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

‼ MySQL Service Observed

We observed MySQL, a database management system, publicly exposed.

-0.2 SCORE IMPACT

1 finding

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
MySQL	-	65.206.30.70	3306	2019-01-23T07:17:56.000Z

RECOMMENDATION

Exposing database services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

MySQL is an open-source database management system (DBMS). DBMSes are intended to store large amounts of information. We observed a MySQL service on the Internet, accessible by the public. DBMSes are attractive targets to attackers due to the data they may contain. An attacker that breaches a DBMS may sell the databases within, use them for blackmail, or employ the information when launching further attacks. A breached database may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

‼ RDP Service Observed

We observed RDP, a remote access service, publicly exposed.

-0.1 SCORE IMPACT

1 finding

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
Microsoft Terminal Services	-	66.193.233.165	3389	2019-01-23T19:09:51.000Z

RECOMMENDATION

Exposing remote access services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The RDP protocol offers remote access to a host, providing a view of the host's console as output and accepting keyboard and mouse events as input. We observed an RDP service on the Internet, accessible by the public. Remote access services are attractive targets to attackers because they provide remote control over a host. Once logged-in, users can install programs, access files, and run commands on the host. Attackers can add hosts over which they have gained control to botnets, adding the host's computational capabilities and bandwidth to their spam, malware, or distributed denial-of-service (DDoS) campaigns. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Due to sharing user authentication databases with other Microsoft services, brute-forcing this service may provide credentials useful on other services. Attackers may launch denial-of-service (DoS) attacks against the service, rendering the service unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

‼ SMB Service Observed

We observed SMB, a file and printer-sharing service, publicly exposed.

-0.2 SCORE IMPACT

4 findings

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
Microsoft Windows Server 2008 R2 - 2012 microsoft-ds	-	184.170.228.66	445	2019-01-18T10:49:38.000Z
Microsoft Windows netbios-ssn	-	184.170.228.66	139	2019-01-14T23:56:38.000Z

Microsoft Windows Server 2008 R2 - 2012 microsoft-ds	-	184.170.225.205	445	2019-01-06T02:54:31.783Z
Banner: \x00\x00\x00\x7f\xffSMBr\x00\x00\x00\x00\x88\x01@\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00@\x06\x00\x00\x01\x00\x11\x07\x00\x032\x00\x01\x00\x04A\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\xfc\xe3\x01\x00\xfa\xa8\xfe$k\xa5\xd4\x01,\x01\x08:\x00\xe4Y\x19\xac\xb4~J\xa7W\x00O\x00R\x00K\x00G\x00R\x00O\x00U\x00P\x00\x00\x00S\x00A\x00L\x00E\x00S\x00D\x00E\x00M\x00O\x00-\x00A\x00P\x00E\x00X\x00\x00\x00				
Microsoft Windows netbios-ssn	-	184.170.225.205	139	2019-01-03T06:40:56.600Z
Banner: \x83\x00\x00\x01\x8f				

RECOMMENDATION

Exposing SMB to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The SMB protocol offers access to files, printers, and other services on a network. We observed an SMB service on the Internet, accessible by the public. These services are attractive targets to attackers due to the data they may contain, and the potential for access to other network resources. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Due to sharing user authentication databases with other Microsoft services, brute-forcing this service may provide credentials useful on other services. Attackers may launch denial-of-service (DoS) attacks against the service, rendering the service unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

NETWORK SECURITY > ISSUE DETAIL

‼ Certificate Is Expired

Expired certificates prevent TLS clients from connecting to servers.

-0.6 SCORE IMPACT

81 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
pacific-uat.hepsiian.com	GeoTrust, Inc.	2013-04-15T16:10:14.000Z	2015-04-18T17:11:51.000Z	64.149.172.189	443
morasp-btat1.fiservapps.com	GeoTrust Inc.	2017-01-11T00:00:00.000Z	2019-01-11T23:59:59.000Z	166.73.13.176	443
morasp-btat1.fiservapps.com	GeoTrust Inc.	2017-01-11T00:00:00.000Z	2019-01-11T23:59:59.000Z	166.73.13.179	443
mycheckfree-alpha.nc.checkfree.com	GeoTrust Inc.	2016-02-22T00:00:00.000Z	2018-02-21T23:59:59.000Z	208.11.141.91	443
alpha-merchantselfcare.checkfree.com	Equifax	2008-10-17T14:35:55.000Z	2010-11-17T15:35:55.000Z	208.11.141.178	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

www.fiserv.com	GeoTrust Inc.	2016-09-19T00:00:00.000Z	2018-09-19T23:59:59.000Z	205.216.53.145	443
cert-aps.checkfree.com	GeoTrust Inc.	2016-02-09T00:00:00.000Z	2018-02-08T23:59:59.000Z	198.246.154.178	443
*.lending.fiservapps.com	GeoTrust, Inc.	2013-09-04T11:10:54.000Z	2017-09-06T05:06:26.000Z	198.246.154.33	443
datadelivery-alt-cert.onefiserv.com	Trustwave Holdings, Inc.	2014-04-18T11:56:00.000Z	2016-04-18T17:56:00.000Z	12.168.132.15	443
connectdublin.checkfree.com	GeoTrust, Inc.	2013-08-25T18:37:44.000Z	2015-09-28T05:29:27.000Z	12.16.164.14	443
di-ib-server.hepsiian.com	GeoTrust Inc.	2016-09-13T00:00:00.000Z	2018-09-13T23:59:59.000Z	64.149.172.214	443
achcpo-corp-uat.fiservapps.com	GeoTrust Inc.	2016-04-13T00:00:00.000Z	2018-04-13T23:59:59.000Z	192.131.76.196	443
mcom-asp-btat.onefiserv.com	GeoTrust Inc.	2016-09-21T00:00:00.000Z	2018-09-21T23:59:59.000Z	192.131.76.59	443
*.lending.fiservapps.com	GeoTrust, Inc.	2013-09-04T11:10:54.000Z	2017-09-06T05:06:26.000Z	192.131.76.225	443
mobilitiapps-btat2.mybills.com	GeoTrust, Inc.	2014-04-28T22:58:17.000Z	2016-05-30T16:58:17.000Z	192.131.76.78	443
mcom-asp-btat.onefiserv.com	GeoTrust Inc.	2016-09-21T00:00:00.000Z	2018-09-21T23:59:59.000Z	192.131.76.62	443
av-billerdirectui-btat.onefiserv.com	Trustwave Holdings, Inc.	2015-05-07T06:07:54.000Z	2017-05-08T12:07:54.000Z	192.131.76.106	443
mcom-asp-btat.onefiserv.com	GeoTrust Inc.	2016-09-21T00:00:00.000Z	2018-09-21T23:59:59.000Z	192.131.76.61	443
cardvalet-ws.fiservapps.com	GeoTrust Inc.	2016-01-08T00:00:00.000Z	2018-01-07T23:59:59.000Z	50.58.9.223	443
billerops-alpha.nc.checkfree.com	GeoTrust, Inc.	2012-02-20T07:32:54.000Z	2014-02-21T20:40:55.000Z	208.11.141.74	443
alpha-aps.checkfree.com	GeoTrust Inc.	2015-11-13T00:00:00.000Z	2017-11-12T23:59:59.000Z	208.11.141.128	443
billerops-beta.nc.checkfree.com	GeoTrust, Inc.	2012-04-08T20:46:41.000Z	2014-04-12T04:43:20.000Z	208.11.141.77	443
sponsorcare-alpha.nc.checkfree.com	GeoTrust Inc.	2016-02-02T00:00:00.000Z	2018-02-01T23:59:59.000Z	208.11.141.73	443
beta-yes.checkfree.com	Equifax	2008-08-19T15:22:11.000Z	2010-10-19T15:22:11.000Z	208.11.141.177	443
bofa-alpha.nc.checkfree.com	GeoTrust Inc.	2016-02-22T00:00:00.000Z	2018-02-21T23:59:59.000Z	208.11.141.157	443
adapters-	GeoTrust Inc.	2016-05-	2018-05-	208.11.141.84	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

alpha.nc.checkfree.com		26T00:00:00.000Z	26T23:59:59.000Z		
ebilldetaildownload-beta.nc.checkfree.com	Checkfree Corp.	2006-03-22T19:40:35.000Z	2011-03-21T19:40:35.000Z	208.11.141.167	443
sgpgw02.cbs.fiserv.com	GeoTrust Inc.	2016-10-26T00:00:00.000Z	2018-10-26T23:59:59.000Z	203.120.42.194	443
*.billmatrix.com	BMC Production	2016-01-07T20:01:31.000Z	2018-09-17T17:21:56.000Z	166.73.102.182	443
monetise-services.onefiserv.com	GeoTrust, Inc.	2014-10-13T11:29:40.000Z	2016-11-13T23:02:04.000Z	208.235.248.43	443
*.billmatrix.com	BMC Production	2016-01-07T20:01:31.000Z	2018-09-17T17:21:56.000Z	166.73.102.190	443
connectdublin.checkfree.com	GeoTrust, Inc.	2013-08-25T18:37:44.000Z	2015-09-28T05:29:27.000Z	12.16.164.65	443
dr.fiservipvpn.com	Symantec Corporation	2015-03-27T00:00:00.000Z	2016-03-27T23:59:59.000Z	65.213.167.2	443
billerdirect.onefiserv.com	GeoTrust, Inc.	2014-04-13T01:50:37.000Z	2015-07-29T06:06:06.000Z	64.128.99.48	443
iclyncpool01.corp.checkfree.com	GeoTrust, Inc.	2012-06-10T08:28:05.000Z	2016-06-12T08:10:33.000Z	204.95.150.234	443
datadelivery-cert.onefiserv.com	GeoTrust, Inc.	2015-04-06T15:14:30.000Z	2016-06-07T16:50:11.000Z	12.168.132.202	443
mmscts-beta.checkfree.com	GeoTrust, Inc.	2012-03-11T23:20:27.000Z	2014-03-15T13:42:38.000Z	12.168.133.87	443
achasp1-btat2.fiserv.com	Trustwave Holdings, Inc.	2014-12-09T04:49:01.000Z	2016-12-08T10:49:01.000Z	12.168.133.174	443
mcc-tgo01-btat2.mybills.com	GeoTrust Inc.	2016-06-14T00:00:00.000Z	2018-06-14T23:59:59.000Z	12.168.133.240	443
mcc-tgo01-btat2.mybills.com	GeoTrust Inc.	2016-06-14T00:00:00.000Z	2018-06-14T23:59:59.000Z	12.168.133.236	443
dit1-cardvalet-m.fiservapps.com	GeoTrust Inc.	2015-12-11T00:00:00.000Z	2017-12-10T23:59:59.000Z	166.73.13.211	443
dit1-cardvalet-ws.fiservapps.com	GeoTrust Inc.	2015-12-11T00:00:00.000Z	2017-12-10T23:59:59.000Z	166.73.13.212	443
dit1-cardvalet-mobiliti.fiservapps.com	GeoTrust Inc.	2015-12-11T00:00:00.000Z	2017-12-10T23:59:59.000Z	166.73.13.210	443
mobile-lic01-uat.fiservapps.com	GeoTrust Inc.	2016-03-11T00:00:00.000Z	2018-03-11T23:59:59.000Z	166.73.13.93	443
services1.fiserv.com	GeoTrust, Inc.	2015-04-15T06:42:25.000Z	2016-05-17T01:23:06.000Z	50.58.9.181	443
merchantselfcare.checkfree.com	GeoTrust Inc.	2016-10-24T00:00:00.000Z	2018-10-24T23:59:59.000Z	63.251.77.66	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

*.onefiserv.com	GeoTrust Inc.	2016-01-12T00:00:00.000Z	2018-01-11T23:59:59.000Z	64.128.99.136	443
services-prod.onefiserv.com	GeoTrust Inc.	2016-03-24T00:00:00.000Z	2018-03-24T23:59:59.000Z	64.128.99.151	443
*.onefiserv.com	GeoTrust Inc.	2016-01-12T00:00:00.000Z	2018-01-11T23:59:59.000Z	64.128.99.68	443
merchantselfcare.checkfree.com	GeoTrust Inc.	2016-10-24T00:00:00.000Z	2018-10-24T23:59:59.000Z	64.128.99.84	443
webmail.fiserv.net	GeoTrust, Inc.	2012-04-10T09:02:40.000Z	2017-01-13T20:39:20.000Z	204.95.150.230	443
*.billmatrix.com	BMC Production	2016-01-07T20:01:31.000Z	2018-09-17T17:21:56.000Z	166.73.156.142	443
*.billmatrix.com	BMC Production	2016-01-07T20:01:31.000Z	2018-09-17T17:21:56.000Z	166.73.156.150	443
qc-emoney.checkfree.com	GeoTrust Inc.	2015-06-10T00:00:00.000Z	2017-06-09T23:59:59.000Z	208.11.141.192	443
wbp321-beta.nc.checkfree.com	Checkfree Corp.	2003-11-04T19:48:18.000Z	2003-12-04T19:48:18.000Z	208.11.141.196	443
onboardadvisor.app.fiserv.com	GeoTrust Inc.	2016-07-19T00:00:00.000Z	2018-07-19T23:59:59.000Z	50.58.9.141	443
download-secure.wealthmanagementbackup.fiserv.com	GeoTrust, Inc.	2013-12-07T05:09:02.000Z	2016-01-08T22:13:59.000Z	209.211.226.237	443
secure.wealthmanagementbackup.fiserv.com	GeoTrust, Inc.	2013-11-16T13:20:32.000Z	2016-01-18T06:03:12.000Z	209.211.226.236	443
proposalgenerationmanager.fiservapps.com	Trustwave Holdings, Inc.	2015-05-18T06:50:18.000Z	2017-05-17T12:50:18.000Z	170.90.16.202	443
connectnorcross.fiserv.com	GeoTrust, Inc.	2010-08-24T09:07:00.000Z	2012-09-24T21:23:22.000Z	204.95.150.47	443
mcom-asp-btat.onefiserv.com	GeoTrust Inc.	2016-09-21T00:00:00.000Z	2018-09-21T23:59:59.000Z	192.131.76.58	443
mcom-asp-btat.onefiserv.com	GeoTrust Inc.	2016-09-21T00:00:00.000Z	2018-09-21T23:59:59.000Z	192.131.76.60	443
director-ipad-qa.fiservapps.com	GeoTrust, Inc.	2013-10-24T14:06:12.000Z	2015-10-27T09:22:58.000Z	192.131.76.40	443
mcom-asp-btat.onefiserv.com	GeoTrust Inc.	2016-09-21T00:00:00.000Z	2018-09-21T23:59:59.000Z	192.131.76.57	443
snap2pay-uat.onefiserv.com	GeoTrust Inc.	2015-09-25T00:00:00.000Z	2017-09-24T23:59:59.000Z	192.131.76.47	443
ls-copui-	Fiserv, Inc.	2016-02-	2018-02-	192.131.76.33	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

uat2.onefiserv.com		09T00:00:00.000Z	09T23:59:59.000Z		
*.onefiserv.com	GeoTrust Inc.	2016-01-12T00:00:00.000Z	2018-01-11T23:59:59.000Z	192.131.46.180	443
b2b.elending.fiservlendingsolutions.com	GeoTrust Inc.	2015-09-18T00:00:00.000Z	2017-09-17T23:59:59.000Z	192.131.46.150	443
www.bankintelligence.fiserv.com	Symantec Corporation	2015-06-01T00:00:00.000Z	2018-05-26T23:59:59.000Z	64.74.244.77	443
*.fiservapps.com	GeoTrust Inc.	2015-06-23T00:00:00.000Z	2017-06-22T23:59:59.000Z	209.163.213.156	443
partnercare-beta.nc.checkfree.com	GeoTrust, Inc.	2012-09-13T06:17:38.000Z	2014-09-15T10:41:24.000Z	208.11.141.88	443
reports.checkfree.com	Equifax	2006-05-18T16:10:44.000Z	2008-05-18T16:10:44.000Z	12.16.165.87	443
monetise-services.onefiserv.com	GeoTrust, Inc.	2014-10-13T11:29:40.000Z	2016-11-13T23:02:04.000Z	12.16.165.142	443
oa-mc-dr.onefiserv.com	GeoTrust, Inc.	2012-02-26T21:34:09.000Z	2014-03-01T08:28:56.000Z	12.16.165.108	443
*.fiservse.com	GlobalSign nv-sa	2015-08-28T17:01:02.000Z	2017-08-28T17:01:02.000Z	65.210.130.84	443
*.onefiserv.com	GeoTrust Inc.	2016-01-12T00:00:00.000Z	2018-01-11T23:59:59.000Z	12.16.165.109	443
pacific-uat.hepsiian.com	GeoTrust, Inc.	2013-04-15T16:10:14.000Z	2015-04-18T17:11:51.000Z	64.149.172.133	443
services1.fiserv.com	GeoTrust Inc.	2016-04-01T00:00:00.000Z	2018-04-01T23:59:59.000Z	64.128.99.60	443
uhgapps.hepsiian.com	GeoTrust, Inc.	2013-09-08T18:04:31.000Z	2015-11-10T18:09:52.000Z	64.149.172.162	443
nascodrs.hepsiian.com	GeoTrust Inc.	2015-11-20T00:00:00.000Z	2017-11-19T23:59:59.000Z	64.149.171.19	443
*.fiservse.com	GlobalSign nv-sa	2015-08-28T17:01:02.000Z	2017-08-28T17:01:02.000Z	65.210.130.82	443

RECOMMENDATION

Services presenting expired certificates should cause noticeable failures, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate, while ensuring the clients that use the service are configured to validate certificates when making TLS connections. If the clients were configured to validate certificates, ensure that their errors are monitored. Evaluate the organization's certificate management policy to ensure that certificates are renewed or decommissioned prior to their expiration date.

ABOUT THIS ISSUE

When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If the certificate a TLS server (e.g., website) presents to a client (e.g., web browser) is outside of those two dates, the client will refuse to connect to the server. Certificates are digital assets that require renewal or decommissioning on a schedule.

NETWORK SECURITY > ISSUE DETAIL

‼ Certificate Is Self-Signed

Servers presenting self-signed certificates trigger warnings in, or prevent connections from TLS clients.

-0.2 SCORE IMPACT

2 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
bac-saml-prod.fiservapps.com	Fiserv	2018-09-13T17:35:23.000Z	2019-09-13T17:35:23.000Z	208.235.248.133	443
efichwaf660a-59.Fiserv.com	Fiserv	2017-12-07T22:05:25.000Z	2020-12-06T22:05:25.000Z	216.138.118.59	443

RECOMMENDATION

Services presenting self-signed certificates should cause noticeable failures or user-visible warnings, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact your CA and arrange issuance of a new certificate, while ensuring the clients that use the service are configured to validate certificates when making TLS connections. If the clients were configured to validate certificates, ensure that their errors are monitored.

ABOUT THIS ISSUE

When a certificate is issued, it is 'signed' by a certificate authority (CA). Signatures are attestations of the certificate-holder's identity. TLS clients (e.g., web browsers) maintain trust stores, which are lists of CAs whose attestations they trust. The ability to sign a certificate may be delegated from a CA to another entity, such as a subsidiary, creating chains of attestations. In the context of chains of attestation, the delegating CA is the root CA, and the delegated CA is the intermediate CA. Trust stores in TLS clients may contain both intermediate and root CAs. TLS clients validate a server's certificate by tracing its chain of attestations back to a CA in its trust store. Certificates that are self-signed have no chain of attestations: they are self-attested. This means that most TLS clients, when presented with a self-signed certificate, will display a warning before connecting to the server, or refuse to connect to the server. Off-the-shelf software and hardware frequently runs services that use self-signed certificates by default. Many of these services can be configured to use certificates that are not self-signed. The use of self-signed certificates may result in TLS clients being configured to skip validating certificates, making their connections vulnerable to man-in-the-middle attacks. Users that bypass their web browser's warning upon connecting to a server presenting a self-signed certificate are also vulnerable to man-in-the-middle attacks. Self-signed certificates have narrow, but legitimate use cases, such as protecting services whose clients are configured to use public key pinning.

NETWORK SECURITY > ISSUE DETAIL

‼ SSL Certificate Uses Weak Signature

TLS analysis reveals a weak signature algorithms, using SHA1 or MD5.

-0.7 SCORE

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IMPACT

24 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
*.lending.fiservapps.com	GeoTrust, Inc.	2013-09-04T11:10:54.000Z	2017-09-06T05:06:26.000Z	198.246.154.33	443
connectdublin.checkfree.com	GeoTrust, Inc.	2013-08-25T18:37:44.000Z	2015-09-28T05:29:27.000Z	12.16.164.65	443
connectnorcross.fiserv.com	GeoTrust, Inc.	2010-08-24T09:07:00.000Z	2012-09-24T21:23:22.000Z	204.95.150.47	443
ebilldetaildownload-beta.nc.checkfree.com	Checkfree Corp.	2006-03-22T19:40:35.000Z	2011-03-21T19:40:35.000Z	208.11.141.167	443
connectdublin.checkfree.com	GeoTrust, Inc.	2013-08-25T18:37:44.000Z	2015-09-28T05:29:27.000Z	12.16.164.14	443
*.billmatrix.com	BMC Production	2016-01-07T20:01:31.000Z	2018-09-17T17:21:56.000Z	166.73.156.142	443
billerops-alpha.nc.checkfree.com	GeoTrust, Inc.	2012-02-20T07:32:54.000Z	2014-02-21T20:40:55.000Z	208.11.141.74	443
services1.fiserv.com	GeoTrust, Inc.	2015-04-15T06:42:25.000Z	2016-05-17T01:23:06.000Z	50.58.9.181	443
pacific-uat.hepsiian.com	GeoTrust, Inc.	2013-04-15T16:10:14.000Z	2015-04-18T17:11:51.000Z	64.149.172.189	443
download-secure.wealthmanagementbackup.fiserv.com	GeoTrust, Inc.	2013-12-07T05:09:02.000Z	2016-01-08T22:13:59.000Z	209.211.226.237	443
oa-mc-dr.onefiserv.com	GeoTrust, Inc.	2012-02-26T21:34:09.000Z	2014-03-01T08:28:56.000Z	12.16.165.108	443
pacific-uat.hepsiian.com	GeoTrust, Inc.	2013-04-15T16:10:14.000Z	2015-04-18T17:11:51.000Z	64.149.172.133	443
reports.checkfree.com	Equifax	2006-05-18T16:10:44.000Z	2008-05-18T16:10:44.000Z	12.16.165.87	443
alpha-merchantselfcare.checkfree.com	Equifax	2008-10-17T14:35:55.000Z	2010-11-17T15:35:55.000Z	208.11.141.178	443
billerdirect.onefiserv.com	GeoTrust, Inc.	2014-04-13T01:50:37.000Z	2015-07-29T06:06:06.000Z	64.128.99.48	443
monetise-services.onefiserv.com	GeoTrust, Inc.	2014-10-13T11:29:40.000Z	2016-11-13T23:02:04.000Z	12.16.165.142	443
uhgapps.hepsiian.com	GeoTrust, Inc.	2013-09-08T18:04:31.000Z	2015-11-10T18:09:52.000Z	64.149.172.162	443
monetise-	GeoTrust, Inc.	2014-10-	2016-11-	208.235.248.43	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

services.onefiserv.com		13T11:29:40.000Z	13T23:02:04.000Z		
mmscts-beta.checkfree.com	GeoTrust, Inc.	2012-03-11T23:20:27.000Z	2014-03-15T13:42:38.000Z	12.168.133.87	443
*.billmatrix.com	BMC Production	2016-01-07T20:01:31.000Z	2018-09-17T17:21:56.000Z	166.73.102.182	443
*.lending.fiservapps.com	GeoTrust, Inc.	2013-09-04T11:10:54.000Z	2017-09-06T05:06:26.000Z	192.131.76.225	443
beta-yes.checkfree.com	Equifax	2008-08-19T15:22:11.000Z	2010-10-19T15:22:11.000Z	208.11.141.177	443
webmail.fiserv.net	GeoTrust, Inc.	2012-04-10T09:02:40.000Z	2017-01-13T20:39:20.000Z	204.95.150.230	443
director-ipad-qa.fiservapps.com	GeoTrust, Inc.	2013-10-24T14:06:12.000Z	2015-10-27T09:22:58.000Z	192.131.76.40	443

RECOMMENDATION

Contact the authority that manages your SSL Certification to ensure that you have an updated signature–such as SHA-2.

ABOUT THIS ISSUE

The integrity of the signature hash algorithm used in signing a certificate is a critical element in the security of the certificate. Weaknesses in hash algorithms can lead to situations in which attackers can obtain fraudulent certificates. The MD5 signature has long been considered outdated by cryptographic specialists. SHA-1 is outdated and has been phased out by several sources - including Microsoft, Google, and Mozilla as of January 1, 2016.

NETWORK SECURITY > ISSUE DETAIL

‼ TLS Protocol Uses Weak Cipher

TLS analysis reveals a weak cipher either through encryption protocol or public key length.

-0.5 SCORE IMPACT

33 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
dalvdmz37.carreker.com	Symantec Corporation	2017-09-08T00:00:00.000Z	2019-09-09T23:59:59.000Z	209.163.213.137	443
connectdublin.checkfree.com	GeoTrust, Inc.	2013-08-25T18:37:44.000Z	2015-09-28T05:29:27.000Z	12.16.164.65	443
architectbk.onefiserv.com	DigiCert Inc	2018-11-21T00:00:00.000Z	2020-11-21T12:00:00.000Z	184.170.226.96	443
SysAdmin7-Prod.fiservapps.com	DigiCert Inc	2018-08-08T00:00:00.000Z	2020-08-08T12:00:00.000Z	192.131.72.142	443
connectnorcross.fiserv.com	GeoTrust, Inc.	2010-08-24T09:07:00.000Z	2012-09-24T21:23:22.000Z	204.95.150.47	443
*.fiservse.com	GlobalSign nv-sa	2017-06-30T12:36:04.000Z	2020-06-30T12:36:04.000Z	12.168.17.230	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

connectdublin.checkfree.com	GeoTrust, Inc.	2013-08-25T18:37:44.000Z	2015-09-28T05:29:27.000Z	12.16.164.14	443
sydgw01.cbs.fiserv.com	GeoTrust Inc.	2017-01-05T00:00:00.000Z	2019-01-05T23:59:59.000Z	210.50.55.217	443
achcpo-dr.onefiserv.com	DigiCert Inc	2018-08-21T00:00:00.000Z	2020-08-21T12:00:00.000Z	50.58.9.212	443
sgpgw01.cbs.fiserv.com	GeoTrust Inc.	2017-01-05T00:00:00.000Z	2019-01-05T23:59:59.000Z	210.24.157.4	443
*.billmatrix.com	BMC Production	2016-01-07T20:01:31.000Z	2018-09-17T17:21:56.000Z	166.73.156.142	443
orlgw01.cbs.fiserv.com	GeoTrust Inc.	2017-01-05T00:00:00.000Z	2019-01-05T23:59:59.000Z	205.160.248.202	443
nyl.hepsiian.com	DigiCert Inc	2018-03-07T00:00:00.000Z	2020-03-07T12:00:00.000Z	64.149.172.70	443
sgpgw01.cbs.fiserv.com	GeoTrust Inc.	2017-01-05T00:00:00.000Z	2019-01-05T23:59:59.000Z	210.24.157.3	443
download-secure.wealthmanagementbackup.fiserv.com	GeoTrust, Inc.	2013-12-07T05:09:02.000Z	2016-01-08T22:13:59.000Z	209.211.226.237	443
secure.wealthmanagementbackup.fiserv.com	Symantec Corporation	2017-05-15T00:00:00.000Z	2019-05-16T23:59:59.000Z	50.58.9.169	443
reports.checkfree.com	Equifax	2006-05-18T16:10:44.000Z	2008-05-18T16:10:44.000Z	12.16.165.87	443
otms.fiserv.com	DigiCert Inc	2018-08-17T00:00:00.000Z	2020-08-17T12:00:00.000Z	63.128.95.117	443
sydgw01.cbs.fiserv.com	GeoTrust Inc.	2017-01-05T00:00:00.000Z	2019-01-05T23:59:59.000Z	210.50.55.210	443
www.rbscashorderts.fiserv.com	Symantec Corporation	2017-04-04T00:00:00.000Z	2019-04-05T23:59:59.000Z	204.97.230.108	443
achrwa.checkfree.com	DigiCert Inc	2018-01-03T00:00:00.000Z	2020-01-04T12:00:00.000Z	12.16.165.127	443
secure.wealthmanagementprimary.fiserv.com	Symantec Corporation	2017-05-17T00:00:00.000Z	2019-05-18T23:59:59.000Z	166.73.6.60	443
awdmg.fiserv.com	DigiCert Inc	2018-01-23T00:00:00.000Z	2020-01-24T12:00:00.000Z	50.58.10.132	443
ondemand.fiserv.com	DigiCert Inc	2017-12-14T00:00:00.000Z	2019-12-15T12:00:00.000Z	204.95.150.37	443
awmag.fiserv.com	DigiCert Inc	2018-01-23T00:00:00.000Z	2020-01-24T12:00:00.000Z	204.95.150.239	443
awseg.fiserv.com	DigiCert Inc	2018-01-23T00:00:00.000Z	2020-01-24T12:00:00.000Z	204.95.150.240	443
SFTM2.Premier.Fiserv	DigiCert Inc	2018-04-	2020-04-	192.131.55.67	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

.com		27T00:00:00.000Z	27T12:00:00.000Z		
lnkvpn.fiserv.com	Symantec Corporation	2017-01-26T00:00:00.000Z	2020-01-27T23:59:59.000Z	98.19.116.50	443
SFTM.Premier.Fiserv.com	Symantec Corporation	2017-07-17T00:00:00.000Z	2019-07-18T23:59:59.000Z	192.131.55.66	443
otms.fiserv.com	DigiCert Inc	2018-08-17T00:00:00.000Z	2020-08-17T12:00:00.000Z	205.219.236.229	443
*.fiservapps.com	Symantec Corporation	2017-07-10T00:00:00.000Z	2019-07-11T23:59:59.000Z	166.73.6.105	443
director-ipad-qa.fiservapps.com	GeoTrust, Inc.	2013-10-24T14:06:12.000Z	2015-10-27T09:22:58.000Z	192.131.76.40	443
longw01.cbs.fiserv.com	GeoTrust Inc.	2017-01-05T00:00:00.000Z	2019-01-05T23:59:59.000Z	89.197.167.78	443

RECOMMENDATION

It is recommended to configure the server to only support strong symmetric ciphers and to use sufficiently large public key sizes. Specifically, avoid RC4 encryption as there have been multiple vulnerabilities discovered that render it insecure. Additionally, it is recommended to use a public key size of more than 2048 bits.

ABOUT THIS ISSUE

The TLS cryptographic configuration being used could be defeated. A symmetric cipher suite is specified by an encryption protocol (e.g. DES, AES). The strength of the encryption used within a Transport Layer Security (TLS) session is determined by the encryption symmetric cipher negotiated between the server and the browser. In order to ensure that only strong cryptographic ciphers are selected the server must be modified to disable the use of weak ciphers and to configure the ciphers in an adequate order. Additionally, as part of the TLS handshake, an asymmetric cipher is utilized. The strength of the asymmetric cipher may be weakened if an insufficient key size is selected.

NETWORK SECURITY > ISSUE DETAIL

FTP Service Observed

We observed FTP, a file-sharing service, publicly exposed.

-0.1 SCORE IMPACT

51 findings

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
oftpd	-	198.167.0.222	990	2019-01-20T16:34:41.000Z
oftpd	-	198.167.0.71	990	2019-01-20T16:34:01.000Z
oftpd	-	198.167.0.175	990	2019-01-20T16:32:44.000Z
oftpd	-	198.167.0.172	990	2019-01-20T16:31:39.000Z
oftpd	-	198.167.0.223	990	2019-01-20T16:31:30.000Z
oftpd	-	198.167.0.25	990	2019-01-20T16:24:59.000Z
oftpd	-	198.167.0.173	990	2019-01-20T16:17:31.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

oftpd	-	198.167.0.73	990	2019-01-20T16:16:48.000Z
oftpd	-	198.167.0.171	990	2019-01-20T15:37:05.000Z
oftpd	-	198.167.0.72	990	2019-01-20T15:36:43.000Z
oftpd	-	198.167.0.51	990	2019-01-20T15:11:57.000Z
oftpd	-	198.167.0.72	21	2019-01-12T20:49:31.100Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.25	21	2019-01-12T20:37:01.486Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.64	21	2019-01-12T20:24:58.142Z
Banner: 220 Service ready for new user.\r\n				
-	-	65.213.167.45	21	2019-01-12T20:20:04.143Z
Banner: 220-Welcome to qa.ftp.ipsfiserv.com\r\n220-This is a private computer system. Access is restricted to users with\r\n220-proper authorization by Fiserv and its affiliates. Authorized users may\r\n220-be restricted to certain functions in accordance with their job\r\n220-responsibilities. Any unauthorized access will be investigated and may\r\n220-be prosecuted to the full extent of the law, including criminal\r\n220 sanctions. If you are not an authorized user, disconnect now.\r\n				
oftpd	-	198.167.0.222	21	2019-01-12T20:00:25.579Z
Banner: 220 Service ready for new user.\r\n				
Microsoft ftpd	-	50.58.8.116	21	2019-01-12T19:31:45.998Z
Banner: 220 Microsoft FTP Service\r\n				
-	-	65.213.167.80	21	2019-01-12T19:24:11.313Z
Banner: 220-Welcome to ftp.ipsfiserv.com\r\n220-This is a private computer system. Access is restricted to users with\r\n220-proper authorization by Fiserv and its affiliates. Authorized users may\r\n220-be restricted to certain functions in accordance with their job\r\n220-responsibilities. Any unauthorized access will be investigated and may\r\n220-be prosecuted to the full extent of the law, including criminal\r\n220 sanctions. If you are not an authorized user, disconnect now.\r\n				
oftpd	-	198.167.0.176	21	2019-01-12T19:08:52.369Z
Banner: 220 Service ready for new user.\r\n				
ProFTPD	-	208.235.248.3	21	2019-01-12T18:03:47.304Z
Banner: 220 65.167.147.52 FTP server ready\r\n				
oftpd	-	198.167.0.223	21	2019-01-12T17:31:35.078Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.175	21	2019-01-12T17:11:59.204Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.179	21	2019-01-12T17:05:57.019Z

Banner: 220 Service ready for new user.\r\n				
Microsoft ftpd	-	50.58.8.117	21	2019-01-12T16:48:41.935Z
Banner: 220 Microsoft FTP Service\r\n				
oftpd	-	198.167.0.63	21	2019-01-12T16:45:25.456Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.65	21	2019-01-12T16:41:03.192Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.180	21	2019-01-12T16:30:04.420Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.67	21	2019-01-12T16:10:38.358Z
Banner: 220 Service ready for new user.\r\n				
Pure-FTPd	-	209.221.136.222	21	2019-01-12T16:07:01.089Z
Banner: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------\r\n220-You are user number 5 of 50 allowed.\r\n220-Local time is now 08:06. Server port: 21.\r\n220-This is a private system - No anonymous login\r\n220-IPv6 connections are also welcome on this server.\r\n220 You will be disconnected after 15 minutes of inactivity.\r\n				
oftpd	-	198.167.0.70	21	2019-01-12T16:05:30.825Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.124	21	2019-01-12T15:54:34.710Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.113	21	2019-01-12T15:32:32.323Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.73	21	2019-01-12T15:23:52.975Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.66	21	2019-01-12T14:59:01.080Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.177	21	2019-01-12T14:51:53.451Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.71	21	2019-01-12T14:19:50.894Z
Banner: 220 Service ready for new user.\r\n				
oftpd	-	198.167.0.174	21	2019-01-12T13:19:41.190Z

Banner: 220 Service ready for new user.\r\n				
Gene6 ftpd	3.10.0 build 2	208.31.22.249	21	2019-01-12T13:16:28.523Z
Banner: 220 Gene6 FTP Server v3.10.0 (Build 2) ready...\r\n				
oftpd	-	198.167.0.65	990	2018-12-20T11:21:30.000Z
oftpd	-	198.167.0.63	990	2018-12-20T11:21:17.000Z
oftpd	-	198.167.0.64	990	2018-12-20T11:18:50.000Z
oftpd	-	198.167.0.10	990	2018-12-20T11:18:41.000Z
-	-	65.213.167.80	990	2018-12-20T11:15:50.000Z
oftpd	-	198.167.0.151	990	2018-12-20T09:24:57.000Z
oftpd	-	198.167.0.113	990	2018-12-20T08:18:02.000Z
oftpd	-	198.167.0.70	990	2018-12-20T08:17:30.000Z
oftpd	-	198.167.0.124	990	2018-12-20T08:17:01.000Z
oftpd	-	198.167.0.174	990	2018-12-20T08:16:55.000Z
Serv-U ftpd	15.1	12.175.11.82	990	2018-12-20T07:29:34.000Z
oftpd	-	198.167.0.67	990	2018-12-20T07:27:24.000Z
oftpd	-	208.74.12.10	990	2018-12-20T06:50:41.000Z

RECOMMENDATION

Review the business necessity of hosting a public FTP server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The FTP protocol offers access to files stored on servers, giving users the ability to upload, download, and delete files. Many FTP servers are used by automated processes, and are neglected or poorly-configured. Modern protocols, such as SFTP, provide better security than FTP. We observed an FTP service on the Internet, accessible by the public. File-sharing services are attractive targets to attackers due to the data they may contain. An attacker that gains access to the files on an FTP server may sell the files within, use them for blackmail, or employ the information when launching further attacks. A breached FTP server may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

NETWORK SECURITY > ISSUE DETAIL

Telnet Service Observed

We observed Telnet, a remote access service, publicly exposed.

-<0.1 SCORE IMPACT

3 findings

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
Cisco router telnetd	-	12.111.185.1	23	2019-01-08T14:51:57.000Z
Cisco router telnetd	-	12.111.185.2	23	2019-01-08T14:51:08.000Z
Cisco router telnetd	-	12.111.185.3	23	2019-01-08T11:48:45.000Z

RECOMMENDATION

Telnet is an inherently unsafe protocol. Remove the service from the Internet. If a remote access service is necessary, replace Telnet with SSH if possible. If not possible, often the case with older networked hardware, ensure the service is only accessible by VPN.

ABOUT THIS ISSUE

Insecure and/or suspicious Telnet open ports have been detected as being publicly accessible. The availability of these ports allow attackers to engage in authentication bypass attacks (such as brute forcing attempts, remote buffer overflows, blank passwords). An attacker can leverage this access to pivot access into further enterprise resources.

NETWORK SECURITY > ISSUE DETAIL

Certificate Lifetime Is Longer Than Best Practices

We observed a certificate with a lifetime longer than 39 Months.

-0.1 SCORE IMPACT

6 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
*.lending.fiservapps.com	GeoTrust, Inc.	2013-09-04T11:10:54.000Z	2017-09-06T05:06:26.000Z	198.246.154.33	443
*.lending.fiservapps.com	GeoTrust, Inc.	2013-09-04T11:10:54.000Z	2017-09-06T05:06:26.000Z	192.131.76.225	443
ebilldetaildownload-beta.nc.checkfree.com	Checkfree Corp.	2006-03-22T19:40:35.000Z	2011-03-21T19:40:35.000Z	208.11.141.167	443
iclyncpool01.corp.checkfree.com	GeoTrust, Inc.	2012-06-10T08:28:05.000Z	2016-06-12T08:10:33.000Z	204.95.150.234	443
webmail.fiserv.net	GeoTrust, Inc.	2012-04-10T09:02:40.000Z	2017-01-13T20:39:20.000Z	204.95.150.230	443
aus-f5-2000b.hs3.hepsiian.com	Fiserv	2015-09-16T20:06:57.000Z	2025-09-13T20:06:57.000Z	64.149.172.32	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

RECOMMENDATION

Contact the CA and arrange the issuance of a new certificate with a lifetime that does not exceed 39 months.

ABOUT THIS ISSUE

When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If the certificate a TLS server (e.g., website) presents to a client (e.g., web browser) is outside of those two dates, the client will refuse to connect to the server. Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. New algorithms and versions of algorithms with larger key sizes are created regularly, and the best practices surrounding certificates evolve with them. The Certificate Authority and Browser forum, an industry group that sets standards surrounding the creation and use of certificates, has decided to limit the lifetime of certificates to 39 months. This means that CAs who are members of the forum are required to issue certificates with lifetimes that do not exceed 39 months.

NETWORK SECURITY > ISSUE DETAIL

TLS Certificate Without Revocation Control

We observed a TLS certificate that did not contain either CRL or OCSP URLs.

-<0.1 SCORE IMPACT

5 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
ebilldetaildownload-beta.nc.checkfree.com	Checkfree Corp.	2006-03-22T19:40:35.000Z	2011-03-21T19:40:35.000Z	208.11.141.167	443
bac-saml-prod.fiservapps.com	Fiserv	2018-09-13T17:35:23.000Z	2019-09-13T17:35:23.000Z	208.235.248.133	443
wbp321-beta.nc.checkfree.com	Checkfree Corp.	2003-11-04T19:48:18.000Z	2003-12-04T19:48:18.000Z	208.11.141.196	443
efichwaf660a-59.Fiserv.com	Fiserv	2017-12-07T22:05:25.000Z	2020-12-06T22:05:25.000Z	216.138.118.59	443
aus-f5-2000b.hs3.hepsiian.com	Fiserv	2015-09-16T20:06:57.000Z	2025-09-13T20:06:57.000Z	64.149.172.32	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

RECOMMENDATION

Contact the CA to request that the certificate be reissued with revocation controls.

ABOUT THIS ISSUE

Certificate revocation lists (CRLs) are files published online by certificate authorities (CAs). These lists indicate which certificates the CA has revoked, invalidating those certificates. TLS clients (e.g., web browsers) may download a CRL, referenced by a TLS server's certificate, to confirm the certificate is currently valid. CAs may operate online certificate status protocol (OCSP) servers, allowing TLS clients to query whether a certificate is currently valid. Responses to OCSP queries may be 'stapled to' (bundled with) certificates by TLS servers. OCSP stapling prevents TLS clients from needing to query the OCSP server themselves, resulting in faster TLS connections. If an attacker acquires the private key corresponding to a certificate, or any other breach of the private key occurs, the CA can use the revocation controls described above to inform TLS clients that the certificate is no longer valid. Certificates that do not contain revocation controls cannot be revoked, and if an attacker acquires the certificate's private key then the certificate will be valid until the expiry date.

NETWORK SECURITY > ISSUE DETAIL

✓ Extended Validation Certificate Observed

The organization has undergone an extended identity-validation process when acquiring a certificate.

17 findings

SUBJECT COMMON NAME	ISSUER ORGANIZATION NAME	NOT VALID BEFORE	NOT VALID AFTER	DESTINATION IP	DESTINATION PORT
www.loancierge.galaxy.app.fiserv.com	DigiCert Inc	2018-02-13T00:00:00.000Z	2020-02-14T12:00:00.000Z	198.246.218.225	443
www.loancierge.galaxy.app.fiserv.com	DigiCert Inc	2018-02-13T00:00:00.000Z	2020-02-14T12:00:00.000Z	198.246.218.224	443
www.loancierge.galaxy.app.fiserv.com	DigiCert Inc	2018-02-13T00:00:00.000Z	2020-02-14T12:00:00.000Z	198.246.218.226	443
www.netbranch.app.fiserv.com	DigiCert Inc	2018-10-04T00:00:00.000Z	2020-10-04T12:00:00.000Z	198.246.218.153	443
www.netbranch.app.fiserv.com	DigiCert Inc	2018-10-04T00:00:00.000Z	2020-10-04T12:00:00.000Z	198.246.218.157	443
www.netbranch.app.fiserv.com	DigiCert Inc	2018-10-04T00:00:00.000Z	2020-10-04T12:00:00.000Z	198.246.218.158	443
www.appscu.fiserv.com	Symantec Corporation	2017-10-19T00:00:00.000Z	2019-10-20T23:59:59.000Z	198.246.218.81	443
www.netbranch.app.fiserv.com	DigiCert Inc	2018-10-04T00:00:00.000Z	2020-10-04T12:00:00.000Z	198.246.218.151	443
www.appscu.fiserv.com	Symantec Corporation	2017-10-19T00:00:00.000Z	2019-10-20T23:59:59.000Z	198.246.218.83	443

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

www.netbranch.app.fiserv.com	DigiCert Inc	2018-10-04T00:00:00.000Z	2020-10-04T12:00:00.000Z	198.246.218.156	443
www.appscu.fiserv.com	Symantec Corporation	2017-10-19T00:00:00.000Z	2019-10-20T23:59:59.000Z	198.246.218.82	443
accountcreate.fiservapps.com	DigiCert Inc	2018-03-15T00:00:00.000Z	2020-03-15T12:00:00.000Z	198.246.218.72	443
www.netbranch.app.fiserv.com	DigiCert Inc	2018-10-04T00:00:00.000Z	2020-10-04T12:00:00.000Z	198.246.218.154	443
www.netbranch.app.fiserv.com	DigiCert Inc	2018-10-04T00:00:00.000Z	2020-10-04T12:00:00.000Z	198.246.218.152	443
accountcreate.fiservapps.com	DigiCert Inc	2018-03-15T00:00:00.000Z	2020-03-15T12:00:00.000Z	198.246.218.70	443
accountcreate.fiservapps.com	DigiCert Inc	2018-03-15T00:00:00.000Z	2020-03-15T12:00:00.000Z	198.246.218.71	443
evcms.hostbyweb.net	GlobalSign nv-sa	2018-03-16T14:26:05.000Z	2019-12-25T14:31:03.000Z	12.168.17.228	443

RECOMMENDATION

EV certificates should be strongly considered by organizations if their users are likely to be targeted by phishing attacks. Phishing attacks often use typosquatted domain names (e.g., exanple.com versus example.com). Users of legitimate sites, who are accustomed to the visual indicators associated with EV certificates are more likely to notice such attacks.

ABOUT THIS ISSUE

Certificate Authorities (CAs) issue certificates according to a variety of policies, and embed within each certificate a reference to the policy under which it was issued. The type of policy that offers the most assurance of the certificate-holder's identity is called an extended validation (EV) policy, and certificates issued under these policies are called EV certificates. To receive an EV certificate, an organization must prove to a CA that it is a currently-operating legal entity, along with several other attributes. EV certificates provide the highest level of assurance currently available. TLS clients (e.g., web browsers) consider EV certificates to be more trustworthy than certificates issued under other policies. Most web browsers display visual indicators a user is viewing a website secured with an EV certificate. Visual indicators provide additional assurance to the user that website they are viewing belongs to the company they intended to visit.

NETWORK SECURITY > ISSUE DETAIL

POP3 Service Observed

We observed POP3, an email retrieval service, publicly exposed.

2 findings

PRODUCT NAME	PRODUCT VERSION	DESTINATION IP	DESTINATION PORT	LAST SEEN
qpopper pop3d	-	208.66.20.24	995	2019-01-21T01:30:06.000Z
Dovecot pop3d	-	209.221.136.222	110	2018-12-25T21:09:08.772Z
Banner: +OK Dovecot ready.\r\n				

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

RECOMMENDATION

Review the business necessity of hosting a public POP3 server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

ABOUT THIS ISSUE

The POP3 protocol offers access to messages stored on email servers. POP3 servers typically contain only the most recent messages received by an email account, deleting the messages from the server once they are downloaded by a user. The use of POP3 may complicate BCP/DR due to each individual user being responsible for the entirety of their email history. We observed a POP3 service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or access the messages within. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

F 51 DNS HEALTH

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

This module measures the health and configuration of a company's DNS settings. It validates that no malicious events occurred in the passive DNS history of the company's network. It also helps validate that mail servers have proper protection in place to avoid spoofing. It also helps verify that DNS servers are configured correctly.

HIGH SEVERITY

Open DNS Resolver Detected	1

MEDIUM SEVERITY

SPF Record Missing	102

LOW SEVERITY

SPF Record Contains a Softfail	5
Malformed SPF Record	0
SPF Record Contains Wildcard	0

✓ POSITIVE SIGNALS

Valid DNSSEC Configuration Detected	0

INFORMATIONAL

There are no Info Risk Issues to detect for DNS Health

DNS HEALTH > ISSUE DETAIL

SPF Record Missing

A missing SPF record has been detected for a domain.

-4.3 SCORE IMPACT

102 findings

DOMAIN	LAST SEEN
fiservcbs.com	2019-01-30T23:51:39.156Z
fiserveft.net	2019-01-30T16:12:32.291Z
fiserveft.org	2019-01-30T16:11:38.752Z
fiserveasyweb.net	2019-01-30T16:11:22.208Z
fiserveft.com	2019-01-30T16:11:08.952Z
fiserveasyweb.com	2019-01-30T16:10:04.711Z
fiserve.com	2019-01-30T16:10:01.449Z
checkfreeweb.com	2019-01-30T15:37:44.766Z
onefiserv.org	2019-01-29T03:00:35.285Z
onefiserv.com	2019-01-29T02:55:31.305Z
fiservservices.info	2019-01-26T06:55:11.563Z
fiservsa2.com	2019-01-26T06:55:11.542Z
fiservdox.com	2019-01-26T06:55:11.494Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

fiservmail.com	2019-01-26T06:55:11.485Z
fiservfg.com	2019-01-26T06:55:11.428Z
zashpayfromfiserv.org	2019-01-26T06:55:10.576Z
fiserv.org	2019-01-26T06:55:10.572Z
zashpay-fiserv.org	2019-01-26T06:55:05.851Z
fiservlending.com	2019-01-26T06:55:04.783Z
fiserv.net	2019-01-26T06:55:04.681Z
fiservfsc.com	2019-01-26T06:55:04.598Z
summitsite.com	2019-01-26T06:55:04.573Z
fiservboston.com	2019-01-26T06:55:04.491Z
fiservcws.com	2019-01-26T06:55:04.033Z
fiservsa4.com	2019-01-26T06:54:28.430Z
fiservsw.com	2019-01-26T06:54:28.399Z
zashpayfromfiserv.info	2019-01-26T06:54:27.588Z
onefiserv.biz	2019-01-26T06:54:27.580Z
zashpaybyfiserv.info	2019-01-26T06:54:27.561Z
efiserv.com	2019-01-26T06:54:27.550Z
fiservip.net	2019-01-26T06:54:27.505Z
fiservsw.net	2019-01-26T06:54:27.473Z
onefiserv.us	2019-01-26T06:54:26.782Z
zashatfiserv.info	2019-01-26T06:54:05.841Z
fiservcsi.info	2019-01-26T06:54:05.645Z
zashpaybyfiserv.mobi	2019-01-26T06:54:04.494Z
fiservla4.com	2019-01-26T06:54:04.487Z
fiservpit.com	2019-01-26T06:54:04.409Z
zashpay-fiserv.info	2019-01-26T06:54:01.736Z
zashatfiserv.mobi	2019-01-26T06:54:00.108Z
fiservvpn.net	2019-01-26T06:50:18.585Z
zashatfiserv.biz	2019-01-26T06:50:18.584Z
fiservcpsclients.com	2019-01-26T06:50:18.532Z
fiservse.com	2019-01-26T06:50:18.429Z
fiservbusiness.com	2019-01-26T06:50:18.351Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

fiservapps.org	2019-01-26T06:50:17.036Z
fiservsupport.com	2019-01-26T06:50:16.952Z
fiservdm.net	2019-01-26T06:50:16.951Z
agiliti-fiserv.com	2019-01-26T06:50:16.951Z
fiservwebsolutions.com	2019-01-26T06:50:16.828Z
fiserverdc.com	2019-01-26T06:50:15.775Z
zashpayfromfiserv.mobi	2019-01-26T06:50:15.774Z
esolutionsfiserv.com	2019-01-26T06:50:15.632Z
fiservsa6.com	2019-01-26T06:50:15.632Z
zashpayfiserv.info	2019-01-26T06:49:04.697Z
fiservdmdr.net	2019-01-26T06:49:04.613Z
zashpayfiserv.net	2019-01-26T06:49:04.269Z
zashpayfiserv.biz	2019-01-26T06:49:04.235Z
zash-fiserv.info	2019-01-26T06:49:04.213Z
fiservdm.info	2019-01-26T06:49:04.020Z
zashpaybyfiserv.biz	2019-01-26T06:49:03.084Z
fiservcreditservices.com	2019-01-26T06:49:03.083Z
fiservsourceone.com	2019-01-26T06:49:03.025Z
fiservservices.org	2019-01-26T06:47:53.340Z
onefiserv.mobi	2019-01-26T06:47:51.179Z
fiservapps.com	2019-01-26T06:47:51.075Z
fiservdirectsource.com	2019-01-26T06:47:51.071Z
fiservsa91.com	2019-01-26T06:47:50.975Z
zashpayfiserv.mobi	2019-01-26T06:47:50.305Z
zashpay-fiserv.biz	2019-01-26T06:47:50.281Z
users.com	2019-01-26T06:47:39.414Z
fiservservices.com	2019-01-26T06:47:39.329Z
agility-fiserv.com	2019-01-26T06:47:39.245Z
fiservsa92.com	2019-01-26T06:47:39.230Z
zashpay-fiserv.mobi	2019-01-26T06:47:38.736Z
fiserv-europe.net	2019-01-26T06:46:45.411Z
zashatfiserv.org	2019-01-26T06:46:45.101Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

fiservinsurance.com	2019-01-26T06:46:44.901Z
fiservls.com	2019-01-26T06:46:42.804Z
zash-fiserv.org	2019-01-26T06:46:42.481Z
fiservoutputsolutions.com	2019-01-26T06:46:41.975Z
fiservatlanta.com	2019-01-26T06:46:41.825Z
mybills.com	2019-01-26T06:46:41.816Z
fiservipvpn.com	2019-01-26T06:46:41.814Z
fiservsa5.com	2019-01-26T06:46:41.800Z
fiservsa3.com	2019-01-26T06:46:41.757Z
zash-fiserv.mobi	2019-01-26T06:46:40.509Z
zash-fiserv.biz	2019-01-26T06:46:40.443Z
hepsiian.com	2019-01-26T06:46:40.344Z
fiservsa93.com	2019-01-26T06:46:40.315Z
zashpaybyfiserv.org	2019-01-26T06:46:38.041Z
fiservlos.com	2019-01-26T06:46:37.897Z
fiservrmd.com	2019-01-26T06:44:35.486Z
fiservip.com	2019-01-26T06:44:35.429Z
zashpayfromfiserv.biz	2019-01-26T06:44:35.396Z
zashpayfiserv.org	2019-01-26T06:44:35.309Z
carreker.com	2019-01-26T06:44:35.199Z
fiservsa1.com	2019-01-26T06:44:35.119Z
fiservlendingsolutions.com	2019-01-26T06:21:47.000Z
fiservlemans.com	2019-01-26T04:56:36.225Z
jeromegroup.com	2019-01-26T04:19:36.293Z
fiserv-galaxy.com	2019-01-26T04:16:50.785Z

RECOMMENDATION

Create a valid Sender Policy Framework (SPF) record. Ensure the configuration of the SPF DNS record to verify syntax and MTA servers. Test the configuration to make sure its valid by checking the header of an incoming email looking for "spf=pass" Allow for DNS caching during testing; it may take up to 48 hours to fully propagate across the Internet. The nature of the SMTP protocol does not allow for complete prevention of spoofed emails, however the SPF header will reveal whether the email is authentic.

ABOUT THIS ISSUE

The Sender Policy Framework (SPF) is a simple but effective email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record is a mechanism that allows a receiving email server to validate that inbound email from a particular domain comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record for that domain in the form of a specially formatted TXT record. An SPF record is required for spoofed e-mail prevention and anti-spam control.

DNS HEALTH > ISSUE DETAIL

SPF Record Contains a Softfail

Softfail attributes in SPF makes spoofing and phishing email possible.

-1.6 SCORE IMPACT

5 findings

DOMAIN	RECORD	ANALYSIS	LAST SEEN
checkfree.com	v=spf1 a:mailout.checkfree.com a:outbd-pstfx.customercenter.net a:mail.apsnet.com a:mail2.checkfree.com a:mail1.checkfree.com a:mail09.rm04.net a:mailout-oh.checkfree.com a:outbd-pstfx-oh.customercenter.net ip4:204.95.150.228 ip4:12.145.177.240 ~all	-	2019-01-30T15:37:27.046Z
pcsbanking.com	-	-	2019-01-26T06:55:04.783Z
fiservatlanta.net	v=spf1 a mx ~all	-	2019-01-26T06:54:27.643Z
fiserv.com	v=spf1 include:_spf1.fiserv.com include:_spf2.fiserv.com include:_spf3.fiserv.com ~all	-	2019-01-26T06:47:53.557Z
fiserv-ecomhosting.com	v=spf1 ip4:166.73.19.0/24 ip4:12.145.177.0/24 ip4:12.16.164.60 ip4:204.95.150.32 a mx a:phantom.cusa.com ~all	-	2019-01-08T22:31:57.833Z

RECOMMENDATION

To resolve this issue, enumerate the list of email servers that are authorized to send email on behalf of the domain. Update the SPF record with the correct email authorization list.

ABOUT THIS ISSUE

The Sender Policy Framework (SPF) is a simple but effective email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record is a mechanism that allows a receiving email server to validate that inbound email from a particular domain comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record for that domain in the form of a specially formatted TXT record. An SPF record is required for spoofed e-mail prevention and anti-spam control. However, if a softfail attribute is included, it is still possible to spoof email from a particular domain. An SPF record has been detected for the domain.

C 76 PATCHING CADENCE

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The Patching Cadence module analyzes how quickly a company reacts to vulnerabilities to measure patching practices. We look at the rate at which it takes a company to remediate and apply patches compared to peers.

!!! HIGH SEVERITY

High-Severity Vulnerability in Last Observation	5
High Severity CVEs Patching Cadence	41

!! MEDIUM SEVERITY

Medium-Severity Vulnerability in Last Observation	382
End-of-Service Product	1
End-of-Life Product	23
Medium Severity CVEs Patching Cadence	738

! LOW SEVERITY

Low Severity CVEs Patching Cadence	0
Low-Severity Vulnerability in Last Observation	0

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Patching Cadence

i INFORMATIONAL

There are no Info Risk Issues to detect for Patching Cadence

PATCHING CADENCE > ISSUE DETAIL

!!! High-Severity Vulnerability in Last Observation

We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.

-0.4 SCORE IMPACT

5 findings

ID	URL	PUBLICATION DATE	DESTINATION IP	DESTINATION PORT	LAST SEEN
CVE-2017-9078	https://nvd.nist.gov/vuln/detail/CVE-2017-9078	2017-05-19	65.206.30.72	22	2019-01-09T11:33:16.785Z
Description: The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.					
CVE-2016-2776	https://nvd.nist.gov/vuln/detail/CVE-2016-2776	2016-09-28	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.					
CVE-2015-5477	https://nvd.nist.gov/vuln/detail/CVE-2015-5477	2015-07-29	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: named in ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries.					
CVE-2014-8500	https://nvd.nist.gov/vuln/detail/CVE-2014-	2014-10-12	64.149.172.30	53	2019-01-01T15:31:06.385Z

	8500				
Description: ISC BIND 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 does not limit delegation chaining, which allows remote attackers to cause a denial of service (memory consumption and named crash) via a large or infinite number of referrals.					
CVE-2015-5722	https://nvd.nist.gov/vuln/detail/CVE-2015-5722	2015-09-04	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone.					

RECOMMENDATION

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

ABOUT THIS ISSUE

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

High Severity CVEs Patching Cadence

High severity vulnerability seen on network more than 30 days after CVE was published.

-0.9 SCORE IMPACT

41 findings

ID	URL	PUBLICATION DATE	DESTINATION IP	DESTINATION PORT	LAST SEEN
CVE-2014-3515	https://nvd.nist.gov/vuln/detail/CVE-2014-3515	2014-07-09	209.163.213.134	443	2018-12-16T13:13:28.000Z
Description: The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.					
CVE-2014-9427	https://nvd.nist.gov/vuln/detail/CVE-2014-9427	2015-01-02	209.163.213.134	443	2018-12-16T13:13:28.000Z
Description: sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.					
CVE-2014-3669	https://nvd.nist.gov/vuln/detail/CVE-2014-3669	2014-10-29	209.163.213.134	443	2018-12-16T13:13:28.000Z
Description: Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the					

unserialize function that triggers calculation of a large length value.					
CVE-2014-3515	https://nvd.nist.gov/vuln/detail/CVE-2014-3515	2014-07-09	209.163.213.134	80	2018-12-11T04:15:36.000Z
Description: The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.					
CVE-2014-3669	https://nvd.nist.gov/vuln/detail/CVE-2014-3669	2014-10-29	209.163.213.134	80	2018-12-11T04:15:36.000Z
Description: Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.					
CVE-2014-9427	https://nvd.nist.gov/vuln/detail/CVE-2014-9427	2015-01-02	209.163.213.134	80	2018-12-11T04:15:36.000Z
Description: sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.					
CVE-2014-9427	https://nvd.nist.gov/vuln/detail/CVE-2014-9427	2015-01-02	12.14.174.237	-	2018-06-20T13:25:54.000Z
Description: sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.					
CVE-2014-9427	https://nvd.nist.gov/vuln/detail/CVE-2014-9427	2015-01-02	12.14.174.237	-	2018-05-19T13:05:22.000Z
Description: sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.					
CVE-2018-6789	https://nvd.nist.gov/vuln/detail/CVE-2018-6789	2018-02-08	209.221.136.222	-	2018-04-20T21:00:15.000Z
Description: An issue was discovered in the base64d function in the SMTP listener in Exim before 4.90.1. By sending a handcrafted message, a buffer overflow may happen. This can be used to execute code remotely.					
CVE-2017-16943	https://nvd.nist.gov/vuln/detail/CVE-2017-16943	2017-11-25	209.221.136.222	-	2018-04-20T21:00:15.000Z
Description: The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via vectors involving BDAT commands.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	198.167.0.48	-	2018-04-19T08:01:30.000Z

Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	198.167.0.17	-	2018-04-19T08:01:30.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.204	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.167	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.196	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.177	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.192	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	192.131.55.82	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.91	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-	2017-06-19	208.11.141.155	-	2018-04-19T04:28:41.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	3167				
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.88	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	192.131.72.203	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.73	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.78	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	192.131.55.83	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.75	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.64	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	208.11.141.132	-	2018-04-19T04:28:41.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	64.128.99.203	-	2018-04-19T02:12:57.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	198.167.0.33	-	2018-04-19T01:35:31.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	198.167.0.248	-	2018-04-19T01:35:31.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	63.240.88.6	-	2018-04-19T01:35:31.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	198.167.0.148	-	2018-04-19T01:35:31.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	198.167.0.246	-	2018-04-19T01:35:31.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	166.73.6.118	-	2018-04-19T01:35:31.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	198.167.0.133	-	2018-04-19T01:35:31.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	64.149.172.15	-	2018-04-17T12:50:05.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	64.149.172.137	-	2018-04-17T12:50:05.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2017-3167	https://nvd.nist.gov/vuln/detail/CVE-2017-3167	2017-06-19	209.163.213.134	-	2018-04-12T19:04:32.000Z
Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.					
CVE-2014-3669	https://nvd.nist.gov/vuln/detail/CVE-2014-3669	2014-10-29	209.163.213.134	-	2018-04-12T19:04:32.000Z
Description: Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.					
CVE-2014-3515	https://nvd.nist.gov/vuln/detail/CVE-2014-3515	2014-07-09	209.163.213.134	-	2018-04-12T19:04:32.000Z
Description: The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.					

RECOMMENDATION

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the BugTraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

ABOUT THIS ISSUE

Based on scan data, the company had high severity CVE vulnerability that was open longer than 30 days after the CVE was published. High severity CVEs are those with a documented CVSS severity over 7.0. It is best practice in standards such as PCI DSS to mitigate or patch high severity vulnerabilities within 30 days. Details on each vulnerability are listed in the table below.

PATCHING CADENCE > ISSUE DETAIL

Medium-Severity Vulnerability in Last Observation

We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.

-0.6 SCORE IMPACT

382 findings

ID	URL	PUBLICATION DATE	DESTINATION IP	DESTINATION PORT	LAST SEEN
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.91	443	2019-01-18T07:44:06.000Z
Description:					

There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.91	443	2019-01-18T07:44:06.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.91	443	2019-01-18T07:44:06.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.91	443	2019-01-18T07:44:06.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.91	443	2019-01-18T07:44:06.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.91	443	2019-01-18T07:44:06.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.91	443	2019-01-18T07:44:06.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	198.246.154.102	443	2019-01-18T04:30:46.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	198.246.154.102	443	2019-01-18T04:30:46.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	198.246.154.102	443	2019-01-18T04:30:46.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	198.246.154.102	443	2019-01-18T04:30:46.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	198.246.154.102	443	2019-01-18T04:30:46.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.246.154.102	443	2019-01-18T04:30:46.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	198.246.154.102	443	2019-01-18T04:30:46.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC					

algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.246	443	2019-01-17T22:12:01.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	192.131.76.193	443	2019-01-17T20:37:00.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.76.193	443	2019-01-17T20:37:00.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	192.131.76.193	443	2019-01-17T20:37:00.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	192.131.76.193	443	2019-01-17T20:37:00.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.76.193	443	2019-01-17T20:37:00.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

<table>
<tr><td>CVE-2017-3736</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3736</td><td>2017-11-02</td><td>192.131.76.193</td><td>443</td><td>2019-01-17T20:37:00.000Z</td></tr>
<tr><td colspan="6">Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>192.131.76.193</td><td>443</td><td>2019-01-17T20:37:00.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-5647</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-5647</td><td>2017-04-17</td><td>208.74.12.10</td><td>443</td><td>2019-01-17T17:11:34.000Z</td></tr>
<tr><td colspan="6">Description:
A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>198.167.0.148</td><td>443</td><td>2019-01-17T16:00:30.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>166.73.14.52</td><td>443</td><td>2019-01-17T14:47:18.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2017-3738</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3738</td><td>2017-12-07</td><td>166.73.14.52</td><td>443</td><td>2019-01-17T14:47:18.000Z</td></tr>
<tr><td colspan="6">Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vu</td><td>2014-07-20</td><td>166.73.14.52</td><td>443</td><td>2019-01-</td></tr>
</table>

	ln/detail/CVE-2014-0226				17T14:47:18.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.14.52	443	2019-01-17T14:47:18.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.14.52	443	2019-01-17T14:47:18.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.14.52	443	2019-01-17T14:47:18.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.14.52	443	2019-01-17T14:47:18.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.14.117	443	2019-01-17T14:47:17.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.14.117	443	2019-01-17T14:47:17.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.14.117	443	2019-01-17T14:47:17.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.14.117	443	2019-01-17T14:47:17.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.14.117	443	2019-01-17T14:47:17.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.14.117	443	2019-01-17T14:47:17.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.14.117	443	2019-01-17T14:47:17.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.13.244	443	2019-01-17T14:40:11.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.13.244	443	2019-01-17T14:40:11.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a					

handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.13.244	443	2019-01-17T14:40:11.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.13.244	443	2019-01-17T14:40:11.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.13.244	443	2019-01-17T14:40:11.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.13.244	443	2019-01-17T14:40:11.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.13.244	443	2019-01-17T14:40:11.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.33	443	2019-01-17T12:44:23.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.177	443	2019-01-17T10:54:06.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.177	443	2019-01-17T10:54:06.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.177	443	2019-01-17T10:54:06.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.177	443	2019-01-17T10:54:06.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.177	443	2019-01-17T10:54:06.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.177	443	2019-01-17T10:54:06.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.177	443	2019-01-17T10:54:06.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a					

private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.78	443	2019-01-17T10:51:31.000Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.78	443	2019-01-17T10:51:31.000Z

Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.78	443	2019-01-17T10:51:31.000Z

Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.78	443	2019-01-17T10:51:31.000Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.78	443	2019-01-17T10:51:31.000Z

Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.78	443	2019-01-17T10:51:31.000Z

Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would

have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.78	443	2019-01-17T10:51:31.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.132	443	2019-01-17T10:50:47.000Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.132	443	2019-01-17T10:50:47.000Z

Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.132	443	2019-01-17T10:50:47.000Z

Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.132	443	2019-01-17T10:50:47.000Z

Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.132	443	2019-01-17T10:50:47.000Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

<table>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>208.11.141.132</td><td>443</td><td>2019-01-17T10:50:47.000Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
<tr><td>CVE-2015-3185</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3185</td><td>2015-07-20</td><td>208.11.141.132</td><td>443</td><td>2019-01-17T10:50:47.000Z</td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>208.11.141.76</td><td>443</td><td>2019-01-17T10:42:47.000Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>208.11.141.76</td><td>443</td><td>2019-01-17T10:42:47.000Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>208.11.141.76</td><td>443</td><td>2019-01-17T10:42:47.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-3738</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3738</td><td>2017-12-07</td><td>208.11.141.76</td><td>443</td><td>2019-01-17T10:42:47.000Z</td></tr>
<tr><td colspan="6">Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.</td></tr>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>208.11.141.76</td><td>443</td><td>2019-01-17T10:42:47.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would</td></tr>
</table>

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.76	443	2019-01-17T10:42:47.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.76	443	2019-01-17T10:42:47.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.167	443	2019-01-17T10:39:06.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.167	443	2019-01-17T10:39:06.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.167	443	2019-01-17T10:39:06.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.167	443	2019-01-17T10:39:06.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.167	443	2019-01-17T10:39:06.000Z
Description:					

<table>
<tr><td colspan="6">The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2017-3736</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3736</td><td>2017-11-02</td><td>208.11.141.167</td><td>443</td><td>2019-01-17T10:39:06.000Z</td></tr>
<tr><td colspan="6">Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</td></tr>
<tr><td>CVE-2017-3738</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3738</td><td>2017-12-07</td><td>208.11.141.167</td><td>443</td><td>2019-01-17T10:39:06.000Z</td></tr>
<tr><td colspan="6">Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.</td></tr>
<tr><td>CVE-2015-3185</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3185</td><td>2015-07-20</td><td>208.11.141.75</td><td>443</td><td>2019-01-17T10:38:27.000Z</td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2016-0703</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-0703</td><td>2016-03-02</td><td>208.11.141.75</td><td>443</td><td>2019-01-17T10:38:27.000Z</td></tr>
<tr><td colspan="6">Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.</td></tr>
<tr><td>CVE-2015-3195</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3195</td><td>2015-12-06</td><td>208.11.141.75</td><td>443</td><td>2019-01-17T10:38:27.000Z</td></tr>
<tr><td colspan="6">Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>208.11.141.75</td><td>443</td><td>2019-01-17T10:38:27.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>208.11.141.75</td><td>443</td><td>2019-01-17T10:38:27.000Z</td></tr>
</table>

Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.75	443	2019-01-17T10:38:27.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.75	443	2019-01-17T10:38:27.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.75	443	2019-01-17T10:38:27.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	199.47.156.89	443	2019-01-17T10:34:10.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	199.47.156.89	443	2019-01-17T10:34:10.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	199.47.156.89	443	2019-01-17T10:34:10.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	199.47.156.89	443	2019-01-17T10:34:10.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on					

<table>
<tr><td colspan="6">TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.</td></tr>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>199.47.156.89</td><td>443</td><td>2019-01-17T10:34:10.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>199.47.156.89</td><td>443</td><td>2019-01-17T10:34:10.000Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>199.47.156.89</td><td>443</td><td>2019-01-17T10:34:10.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-7529</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-7529</td><td>2017-07-13</td><td>66.193.233.167</td><td>443</td><td>2019-01-17T06:34:42.000Z</td></tr>
<tr><td colspan="6">Description:
Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.</td></tr>
<tr><td>CVE-2016-0703</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-0703</td><td>2016-03-02</td><td>63.240.88.6</td><td>443</td><td>2019-01-17T03:20:40.000Z</td></tr>
<tr><td colspan="6">Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>63.240.88.6</td><td>443</td><td>2019-01-17T03:20:40.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>64.128.99.203</td><td>443</td><td>2019-01-17T02:49:38.000Z</td></tr>
</table>

Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	64.128.99.203	443	2019-01-17T02:49:38.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	64.128.99.203	443	2019-01-17T02:49:38.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	64.128.99.203	443	2019-01-17T02:49:38.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	64.128.99.203	443	2019-01-17T02:49:38.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	64.128.99.203	443	2019-01-17T02:49:38.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	64.128.99.203	443	2019-01-17T02:49:38.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	64.128.99.203	443	2019-01-17T02:49:38.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-	2015-07-20	64.128.99.92	443	2019-01-17T02:38:34.000Z

<table>
<tr><td></td><td>3185</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>64.128.99.92</td><td>443</td><td>2019-01-17T02:38:34.000Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
<tr><td>CVE-2015-3197</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3197</td><td>2016-02-14</td><td>64.128.99.92</td><td>443</td><td>2019-01-17T02:38:34.000Z</td></tr>
<tr><td colspan="6">Description:
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>64.128.99.92</td><td>443</td><td>2019-01-17T02:38:34.000Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</td></tr>
<tr><td>CVE-2016-0703</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-0703</td><td>2016-03-02</td><td>64.128.99.92</td><td>443</td><td>2019-01-17T02:38:34.000Z</td></tr>
<tr><td colspan="6">Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.</td></tr>
<tr><td>CVE-2015-3195</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3195</td><td>2015-12-06</td><td>64.128.99.92</td><td>443</td><td>2019-01-17T02:38:34.000Z</td></tr>
<tr><td colspan="6">Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>64.128.99.92</td><td>443</td><td>2019-01-17T02:38:34.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2015-3194</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3194</td><td>2015-12-06</td><td>64.128.99.92</td><td>443</td><td>2019-01-17T02:38:34.000Z</td></tr>
<tr><td colspan="6">Description:
crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.</td></tr>
</table>

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.235.248.176	443	2019-01-17T01:31:10.000Z

Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.235.248.176	443	2019-01-17T01:31:10.000Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.235.248.176	443	2019-01-17T01:31:10.000Z

Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.235.248.176	443	2019-01-17T01:31:10.000Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.235.248.176	443	2019-01-17T01:31:10.000Z

Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.235.248.176	443	2019-01-17T01:31:10.000Z

Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-	2015-07-20	208.235.248.176	443	2019-01-17T01:31:10.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	3183				
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	64.149.172.15	443	2019-01-16T23:07:25.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	64.149.172.15	443	2019-01-16T23:07:25.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	64.149.172.15	443	2019-01-16T23:07:25.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	64.149.172.15	443	2019-01-16T23:07:25.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	64.149.172.15	443	2019-01-16T23:07:25.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	64.149.172.15	443	2019-01-16T23:07:25.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.149.172.15	443	2019-01-16T23:07:25.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					

<table>
<tr><td>CVE-2015-3194</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3194</td><td>2015-12-06</td><td>64.149.172.15</td><td>443</td><td>2019-01-16T23:07:25.000Z</td></tr>
<tr><td colspan="6">Description:
crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>198.167.0.48</td><td>443</td><td>2019-01-16T19:46:07.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2015-3185</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3185</td><td>2015-07-20</td><td>192.131.76.25</td><td>443</td><td>2019-01-16T19:33:07.000Z</td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2017-3736</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3736</td><td>2017-11-02</td><td>192.131.76.25</td><td>443</td><td>2019-01-16T19:33:07.000Z</td></tr>
<tr><td colspan="6">Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>192.131.76.25</td><td>443</td><td>2019-01-16T19:33:07.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>192.131.76.25</td><td>443</td><td>2019-01-16T19:33:07.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>192.131.76.25</td><td>443</td><td>2019-01-16T19:33:07.000Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
</table>

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	192.131.76.25	443	2019-01-16T19:33:07.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.76.25	443	2019-01-16T19:33:07.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	192.131.72.236	443	2019-01-16T18:05:35.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.13.27	443	2019-01-16T17:39:27.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.13.27	443	2019-01-16T17:39:27.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.13.27	443	2019-01-16T17:39:27.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.13.27	443	2019-01-16T17:39:27.000Z

Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.13.27	443	2019-01-16T17:39:27.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.13.27	443	2019-01-16T17:39:27.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.13.27	443	2019-01-16T17:39:27.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.235.248.131	443	2019-01-16T09:44:43.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.235.248.131	443	2019-01-16T09:44:43.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.235.248.131	443	2019-01-16T09:44:43.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.235.248.131	443	2019-01-16T09:44:43.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.235.248.131	443	2019-01-16T09:44:43.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.235.248.131	443	2019-01-16T09:44:43.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.235.248.131	443	2019-01-16T09:44:43.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.235.248.157	443	2019-01-16T09:42:14.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.235.248.157	443	2019-01-16T09:42:14.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-	2015-07-20	208.235.248.157	443	2019-01-16T09:42:14.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	3185				
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.235.248.157	443	2019-01-16T09:42:14.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.235.248.157	443	2019-01-16T09:42:14.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.235.248.157	443	2019-01-16T09:42:14.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.235.248.157	443	2019-01-16T09:42:14.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.235.248.133	443	2019-01-16T09:32:11.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.235.248.133	443	2019-01-16T09:32:11.000Z
Description:					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.235.248.133	443	2019-01-16T09:32:11.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.235.248.133	443	2019-01-16T09:32:11.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.235.248.133	443	2019-01-16T09:32:11.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.235.248.133	443	2019-01-16T09:32:11.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.235.248.133	443	2019-01-16T09:32:11.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.92.88	443	2019-01-16T08:24:14.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-	2017-11-02	166.73.92.88	443	2019-01-16T08:24:14.000Z

	3736				
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.92.88	443	2019-01-16T08:24:14.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.92.88	443	2019-01-16T08:24:14.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.92.88	443	2019-01-16T08:24:14.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.92.88	443	2019-01-16T08:24:14.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.92.88	443	2019-01-16T08:24:14.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.192	443	2019-01-16T07:13:12.000Z
Description:					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.192	443	2019-01-16T07:13:12.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.192	443	2019-01-16T07:13:12.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.192	443	2019-01-16T07:13:12.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.192	443	2019-01-16T07:13:12.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.192	443	2019-01-16T07:13:12.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.192	443	2019-01-16T07:13:12.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.196	443	2019-01-16T07:05:38.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.196	443	2019-01-16T07:05:38.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.196	443	2019-01-16T07:05:38.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.196	443	2019-01-16T07:05:38.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.196	443	2019-01-16T07:05:38.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.196	443	2019-01-16T07:05:38.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-	2014-07-20	208.11.141.196	443	2019-01-16T07:05:38.000Z

	0226				
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.7.11	443	2019-01-16T07:00:56.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.7.11	443	2019-01-16T07:00:56.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.7.11	443	2019-01-16T07:00:56.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.7.11	443	2019-01-16T07:00:56.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.7.11	443	2019-01-16T07:00:56.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.7.11	443	2019-01-16T07:00:56.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.7.11	443	2019-01-16T07:00:56.000Z

Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.6.117	443	2019-01-16T05:41:31.000Z

Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.6.117	443	2019-01-16T05:41:31.000Z

Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.6.117	443	2019-01-16T05:41:31.000Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.6.117	443	2019-01-16T05:41:31.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.6.117	443	2019-01-16T05:41:31.000Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.6.117	443	2019-01-16T05:41:31.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.6.117	443	2019-01-16T05:41:31.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.6.118	443	2019-01-16T05:40:54.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.6.118	443	2019-01-16T05:40:54.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.6.118	443	2019-01-16T05:40:54.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.6.118	443	2019-01-16T05:40:54.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.6.118	443	2019-01-16T05:40:54.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vu	2017-11-02	166.73.6.118	443	2019-01-

	ln/detail/CVE-2017-3736				16T05:40:54.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.6.118	443	2019-01-16T05:40:54.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.88	443	2019-01-16T00:59:46.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.88	443	2019-01-16T00:59:46.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.88	443	2019-01-16T00:59:46.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.88	443	2019-01-16T00:59:46.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.88	443	2019-01-16T00:59:46.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.88	443	2019-01-16T00:59:46.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.88	443	2019-01-16T00:59:46.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	66.193.233.175	80	2019-01-12T21:58:58.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	66.193.233.175	80	2019-01-12T21:58:58.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	66.193.233.175	80	2019-01-12T21:58:58.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-	2015-07-20	66.193.233.175	80	2019-01-12T21:58:58.000Z

<table>
<tr><td></td><td>3185</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>66.193.233.175</td><td>80</td><td>2019-01-12T21:58:58.000Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>66.193.233.175</td><td>80</td><td>2019-01-12T21:58:58.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>66.193.233.175</td><td>80</td><td>2019-01-12T21:58:58.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2014-3566</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-3566</td><td>2014-10-14</td><td>63.128.95.117</td><td>443</td><td>2019-01-12T05:29:55.914Z</td></tr>
<tr><td colspan="6">Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.</td></tr>
<tr><td>CVE-2016-0800</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-0800</td><td>2016-03-01</td><td>205.219.236.229</td><td>443</td><td>2019-01-12T04:56:14.036Z</td></tr>
<tr><td colspan="6">Description:
The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.</td></tr>
<tr><td>CVE-2014-3566</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-3566</td><td>2014-10-14</td><td>205.219.236.229</td><td>443</td><td>2019-01-12T04:56:14.036Z</td></tr>
<tr><td colspan="6">Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.</td></tr>
<tr><td>CVE-2014-3566</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-3566</td><td>2014-10-14</td><td>198.246.154.136</td><td>443</td><td>2019-01-12T02:17:11.556Z</td></tr>
<tr><td colspan="6">Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.</td></tr>
</table>

<table>
<tr><td>CVE-2014-3566</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-3566</td><td>2014-10-14</td><td>12.16.165.127</td><td>443</td><td>2019-01-11T23:45:06.645Z</td></tr>
<tr><td colspan="6">Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.</td></tr>
<tr><td>CVE-2014-3566</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-3566</td><td>2014-10-14</td><td>12.16.164.14</td><td>443</td><td>2019-01-11T23:01:19.002Z</td></tr>
<tr><td colspan="6">Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.</td></tr>
<tr><td>CVE-2014-3566</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-3566</td><td>2014-10-14</td><td>50.58.10.133</td><td>443</td><td>2019-01-11T22:56:32.759Z</td></tr>
<tr><td colspan="6">Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.</td></tr>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>208.11.141.76</td><td>80</td><td>2019-01-11T22:50:41.000Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>208.11.141.76</td><td>80</td><td>2019-01-11T22:50:41.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2017-3738</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3738</td><td>2017-12-07</td><td>208.11.141.76</td><td>80</td><td>2019-01-11T22:50:41.000Z</td></tr>
<tr><td colspan="6">Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>208.11.141.76</td><td>80</td><td>2019-01-11T22:50:41.000Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</td></tr>
</table>

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.76	80	2019-01-11T22:50:41.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.76	80	2019-01-11T22:50:41.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.76	80	2019-01-11T22:50:41.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-7529	https://nvd.nist.gov/vuln/detail/CVE-2017-7529	2017-07-13	66.193.233.167	80	2019-01-11T18:21:17.000Z
Description: Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.76.202	443	2019-01-11T12:45:22.138Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.76.78	443	2019-01-11T12:34:21.489Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.76.203	443	2019-01-11T12:20:21.534Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	50.58.10.161	443	2019-01-10T22:34:40.871Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	50.58.10.165	443	2019-01-10T22:17:34.853Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.168.132.240	443	2019-01-10T21:56:48.732Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.11.141.9	443	2019-01-10T20:16:20.205Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.11.141.38	443	2019-01-10T20:13:49.019Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.73.13	443	2019-01-10T17:25:25.893Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.72.240	443	2019-01-10T17:12:32.162Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.240	443	2019-01-10T16:05:43.264Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.235.248.43	443	2019-01-10T13:48:42.367Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.164.65	443	2019-01-10T13:02:05.566Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for					

man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	184.170.226.96	443	2019-01-10T10:17:20.571Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.48	443	2019-01-10T07:02:03.521Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.44.79.219	443	2019-01-10T04:37:51.960Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	204.95.150.234	443	2019-01-10T04:23:05.368Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.234	443	2019-01-10T04:23:05.368Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.215	443	2019-01-10T03:58:54.250Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	198.246.154.221	443	2019-01-10T00:59:08.126Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.168.132.183	443	2019-01-09T20:49:00.865Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0777	https://nvd.nist.gov/vuln/detail/CVE-2016-0777	2016-04-01	65.206.30.70	22	2019-01-09T18:52:22.131Z

Description:
The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.252	443	2019-01-09T16:47:04.649Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.168.133.81	443	2019-01-09T16:33:20.094Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.72.207	443	2019-01-09T16:10:06.771Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.72.172	443	2019-01-09T16:03:18.186Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.168.133.229	443	2019-01-09T15:56:46.378Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	166.73.13.54	443	2019-01-09T15:27:05.701Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	170.90.16.206	443	2019-01-09T10:29:37.193Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	50.58.9.169	443	2019-01-09T09:51:01.944Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-	2014-10-14	64.128.99.136	443	2019-01-09T06:22:41.590Z

	3566				
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.218	443	2019-01-09T02:59:41.140Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.235.248.86	443	2019-01-09T00:59:37.385Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.235.248.122	443	2019-01-09T00:44:36.592Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.211.226.237	443	2019-01-08T18:21:09.838Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-0204	https://nvd.nist.gov/vuln/detail/CVE-2015-0204	2015-01-08	209.211.226.236	443	2019-01-08T18:20:59.506Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.211.226.236	443	2019-01-08T18:20:59.506Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	166.73.6.60	443	2019-01-08T17:47:48.460Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.47	443	2019-01-08T17:18:18.765Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2015-0204	https://nvd.nist.gov/vuln/detail/CVE-2015-0204	2015-01-08	204.95.150.47	443	2019-01-08T17:18:18.765Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.76.40	443	2019-01-08T16:03:15.734Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.253	443	2019-01-08T15:46:27.220Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	50.58.10.164	443	2019-01-08T14:46:14.351Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	50.58.10.162	443	2019-01-08T14:35:35.293Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	209.163.213.137	443	2019-01-08T10:38:00.297Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.137	443	2019-01-08T10:38:00.297Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.104	443	2019-01-08T10:34:00.415Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.138	443	2019-01-08T10:22:18.470Z

Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.84	443	2019-01-08T04:44:28.564Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-0204	https://nvd.nist.gov/vuln/detail/CVE-2015-0204	2015-01-08	12.16.165.87	443	2019-01-08T04:25:08.223Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-4000	https://nvd.nist.gov/vuln/detail/CVE-2015-4000	2015-05-20	12.16.165.87	443	2019-01-08T04:25:08.223Z
Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.87	443	2019-01-08T04:25:08.223Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.142	443	2019-01-08T04:20:58.102Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.73	80	2019-01-07T01:37:50.238Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.73	80	2019-01-07T01:37:50.238Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.73	80	2019-01-07T01:37:50.238Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL					

pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.73	80	2019-01-07T01:37:50.238Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.73	80	2019-01-07T01:37:50.238Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.73	80	2019-01-07T01:37:50.238Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.73	80	2019-01-07T01:37:50.238Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.73	80	2019-01-07T01:37:50.238Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.88	80	2019-01-06T12:13:29.238Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.88	80	2019-01-06T12:13:29.238Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the					

initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.88	80	2019-01-06T12:13:29.238Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.88	80	2019-01-06T12:13:29.238Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.88	80	2019-01-06T12:13:29.238Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.88	80	2019-01-06T12:13:29.238Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.88	80	2019-01-06T12:13:29.238Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.177	80	2019-01-06T07:21:26.017Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.177	80	2019-01-06T07:21:26.017Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

smuggling, response splitting and cache pollution.

CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.177	80	2019-01-06T07:21:26.017Z

Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.177	80	2019-01-06T07:21:26.017Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.177	80	2019-01-06T07:21:26.017Z

Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.177	80	2019-01-06T07:21:26.017Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.177	80	2019-01-06T07:21:26.017Z

Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.155	80	2019-01-06T04:21:43.905Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3185	https://nvd.nist.gov/vu	2015-07-20	208.11.141.155	80	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	ln/detail/CVE-2015-3185				06T04:21:43.905Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.155	80	2019-01-06T04:21:43.905Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.155	80	2019-01-06T04:21:43.905Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.155	80	2019-01-06T04:21:43.905Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.155	80	2019-01-06T04:21:43.905Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.155	80	2019-01-06T04:21:43.905Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.155	80	2019-01-06T04:21:43.905Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	63.128.95.117	443	2019-01-02T14:22:27.811Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					

CVE-2016-1286	https://nvd.nist.gov/vuln/detail/CVE-2016-1286	2016-03-09	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted signature record for a DNAME record, related to db.c and resolver.c.					
CVE-2016-6170	https://nvd.nist.gov/vuln/detail/CVE-2016-6170	2016-07-06	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: ISC BIND through 9.9.9-P1, 9.10.x through 9.10.4-P1, and 9.11.x through 9.11.0b1 allows primary DNS servers to cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message.					
CVE-2016-8864	https://nvd.nist.gov/vuln/detail/CVE-2016-8864	2016-11-02	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c.					
CVE-2016-1285	https://nvd.nist.gov/vuln/detail/CVE-2016-1285	2016-03-09	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 does not properly handle DNAME records when parsing fetch reply messages, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed packet to the rndc (aka control channel) interface, related to alist.c and sexpr.c.					
CVE-2016-9444	https://nvd.nist.gov/vuln/detail/CVE-2016-9444	2017-01-12	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer.					
CVE-2015-8704	https://nvd.nist.gov/vuln/detail/CVE-2015-8704	2016-01-20	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: apl_42.c in ISC BIND 9.x before 9.9.8-P3, 9.9.x, and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record.					
CVE-2016-9131	https://nvd.nist.gov/vuln/detail/CVE-2016-9131	2017-01-12	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query.					
CVE-2015-8000	https://nvd.nist.gov/vuln/detail/CVE-2015-8000	2015-12-16	64.149.172.30	53	2019-01-01T15:31:06.385Z
Description: db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.					
CVE-2016-0800	https://nvd.nist.gov/vu	2016-03-01	50.58.10.133	443	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	ln/detail/CVE-2016-0800				01T13:10:54.409Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.13.9	443	2018-12-29T15:37:33.193Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.13.9	443	2018-12-29T15:37:33.193Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.13.9	443	2018-12-29T15:37:33.193Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.13.9	443	2018-12-29T15:37:33.193Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.13.9	443	2018-12-29T15:37:33.193Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.13.9	443	2018-12-29T15:37:33.193Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the					

initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.13.9	443	2018-12-29T15:37:33.193Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.73	443	2018-12-29T15:04:59.465Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.73	443	2018-12-29T15:04:59.465Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.73	443	2018-12-29T15:04:59.465Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.73	443	2018-12-29T15:04:59.465Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.73	443	2018-12-29T15:04:59.465Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.73	443	2018-12-29T15:04:59.465Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3183	https://nvd.nist.gov/vu	2015-07-20	208.11.141.73	443	2018-12-

	ln/detail/CVE-2015-3183				29T15:04:59.465Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.73	443	2018-12-29T15:04:59.465Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.92	443	2018-12-29T08:51:43.537Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.92	443	2018-12-29T08:51:43.537Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.92	443	2018-12-29T08:51:43.537Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.92	443	2018-12-29T08:51:43.537Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.92	443	2018-12-29T08:51:43.537Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-	2017-11-02	208.11.141.92	443	2018-12-29T08:51:43.537Z

	3736				
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.92	443	2018-12-29T08:51:43.537Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	192.131.76.23	443	2018-12-29T08:40:33.390Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.76.23	443	2018-12-29T08:40:33.390Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	192.131.76.23	443	2018-12-29T08:40:33.390Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	192.131.76.23	443	2018-12-29T08:40:33.390Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-	2017-11-02	192.131.76.23	443	2018-12-29T08:40:33.390Z

	3736				
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.76.23	443	2018-12-29T08:40:33.390Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.76.23	443	2018-12-29T08:40:33.390Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.204	443	2018-12-29T05:22:32.080Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.204	443	2018-12-29T05:22:32.080Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.204	443	2018-12-29T05:22:32.080Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.204	443	2018-12-29T05:22:32.080Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker					

function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.204	443	2018-12-29T05:22:32.080Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.204	443	2018-12-29T05:22:32.080Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.204	443	2018-12-29T05:22:32.080Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.64	443	2018-12-28T21:53:03.792Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.64	443	2018-12-28T21:53:03.792Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.64	443	2018-12-28T21:53:03.792Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.64	443	2018-12-28T21:53:03.792Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or					

interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.64	443	2018-12-28T21:53:03.792Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.64	443	2018-12-28T21:53:03.792Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.64	443	2018-12-28T21:53:03.792Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.64	443	2018-12-28T21:53:03.792Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.6.220	443	2018-12-17T01:25:40.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.6.220	443	2018-12-17T01:25:40.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.6.220	443	2018-12-17T01:25:40.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.6.220	443	2018-12-17T01:25:40.000Z

Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.6.220	443	2018-12-17T01:25:40.000Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.6.220	443	2018-12-17T01:25:40.000Z

Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.6.220	443	2018-12-17T01:25:40.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

RECOMMENDATION

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

ABOUT THIS ISSUE

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

PATCHING CADENCE > ISSUE DETAIL

End-of-Life Product

We observed an end-of-life product, one that is no longer developed or sold, publicly exposed.

-0.4 SCORE IMPACT

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

23 findings

PRODUCT MANUFACTURER	PRODUCT NAME	PRODUCT VERSION	STATE EFFECTIVE DATE	STATE REF	LAST SEEN	
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-10T21:46:55.862Z	2019-01-17T18:14:29.000Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T18:56:57.235Z	2019-01-16T20:23:14.000Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-10-15T20:23:10.000Z	2019-01-16T20:19:37.000Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-04T12:22:22.792Z	2019-01-10T07:25:23.000Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-10-21T17:24:49.161Z	2018-12-29T18:10:03.589Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T17:41:11.425Z	2018-12-29T16:41:07.480Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T00:17:30.776Z	2018-12-29T16:15:55.619Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T08:02:29.916Z	2018-12-29T15:39:00.441Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-10-21T19:03:57.396Z	2018-12-29T13:47:37.321Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-10T21:41:14.013Z	2018-12-29T11:13:17.297Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-10-22T12:24:39.265Z	2018-12-29T11:00:26.011Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-10-21T21:49:32.979Z	2018-12-29T08:11:04.169Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T02:04:58.648Z	2018-12-29T07:38:03.735Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T04:27:54.419Z	2018-12-29T06:03:07.310Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-10-22T12:26:22.174Z	2018-12-29T04:40:30.253Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-12-29T04:18:57.703Z	2018-12-29T04:18:57.703Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-12-29T03:39:08.542Z	2018-12-29T03:39:08.542Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T13:40:31.260Z	2018-12-28T23:36:23.908Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T01:00:58.279Z	2018-12-28T23:12:54.531Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T02:06:08.110Z	2018-12-28T21:26:34.557Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-09-15T12:55:23.295Z	2018-12-28T21:04:52.428Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-08-11T06:41:41.232Z	2018-12-28T20:36:11.305Z
Microsoft	Internet Information Services 7.0	7.0	2015-01-13	https://support.microsoft.com/en-us/lifecycle?p1=12925	2018-10-22T00:46:02.283Z	2018-12-28T20:35:01.625Z

RECOMMENDATION

Ensure the affected product has an extended support contract that includes security patches. Review the vendor's statement of EOL guidelines for replacement products and upgrade to a new product line or manufacturer.

ABOUT THIS ISSUE

A product that has been declared as end-of-life (EOL) by the manufacturer has been detected. An EOL product is no longer marketed, sold, or upgraded by the manufacturer. Products at this stage in their life cycle are more likely to have vulnerabilities that will remain unpatched.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

PATCHING CADENCE > ISSUE DETAIL

‼ End-of-Service Product

We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed.

-0.1 SCORE IMPACT

1 finding

PRODUCT MANUFACTURER	PRODUCT NAME	PRODUCT VERSION	STATE EFFECTIVE DATE	STATE REF	LAST SEEN	
Juniper	Netscreen SSL Hardware SA2000	-	2016-03-31	http://www.juniper.net/support/eol/ssl_hw.html	2018-10-15T19:15:53.000Z	2019-01-16T05:21:48.000Z

RECOMMENDATION

Replace or upgrade the affected product. Review the vendor's statement of EOS guidelines for replacement products or contact the vendor. In some cases, it may be possible to negotiate a custom support plan for the EOS product.

ABOUT THIS ISSUE

A product that has been declared as end-of-service (EOS) by the manufacturer has been detected. An EOS product is no longer eligible for any support, security patches, or replacement parts. Products at this stage in their life cycle are more likely to have vulnerabilities that need to be patched, but without service support those vulnerabilities will persist until the product is replaced. Using EOS products also violates several compliance frameworks, including PCI DSS and HIPAA.

PATCHING CADENCE > ISSUE DETAIL

‼ Medium Severity CVEs Patching Cadence

Medium severity vulnerability seen on network more than 60 days after CVE was published.

-0.7 SCORE IMPACT

500 findings

ID	URL	PUBLICATION DATE	DESTINATION IP	DESTINATION PORT	LAST SEEN
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.72.203	443	2018-12-16T18:59:11.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	192.131.72.203	443	2018-12-16T18:59:11.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3185	https://nvd.nist.gov/vu	2015-07-20	192.131.72.203	443	2018-12-

	ln/detail/CVE-2015-3185				16T18:59:11.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	192.131.72.203	443	2018-12-16T18:59:11.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	192.131.72.203	443	2018-12-16T18:59:11.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.72.203	443	2018-12-16T18:59:11.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	192.131.72.203	443	2018-12-16T18:59:11.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	192.131.72.203	443	2018-12-16T18:59:11.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-0232	https://nvd.nist.gov/vuln/detail/CVE-2015-0232	2015-01-27	209.163.213.134	443	2018-12-16T13:13:28.000Z
Description: The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	209.163.213.134	443	2018-12-16T13:13:28.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

<table>
<tr><td>CVE-2014-3597</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-3597</td><td>2014-08-22</td><td>209.163.213.134</td><td>443</td><td>2018-12-16T13:13:28.000Z</td></tr>
<tr><td colspan="6">Description:
Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.</td></tr>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>209.163.213.134</td><td>443</td><td>2018-12-16T13:13:28.000Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
<tr><td>CVE-2015-3185</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3185</td><td>2015-07-20</td><td>209.163.213.134</td><td>443</td><td>2018-12-16T13:13:28.000Z</td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>209.163.213.134</td><td>443</td><td>2018-12-16T13:13:28.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2015-3197</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3197</td><td>2016-02-14</td><td>209.163.213.134</td><td>443</td><td>2018-12-16T13:13:28.000Z</td></tr>
<tr><td colspan="6">Description:
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.</td></tr>
<tr><td>CVE-2015-3195</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3195</td><td>2015-12-06</td><td>209.163.213.134</td><td>443</td><td>2018-12-16T13:13:28.000Z</td></tr>
<tr><td colspan="6">Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.</td></tr>
<tr><td>CVE-2014-3670</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-3670</td><td>2014-10-29</td><td>209.163.213.134</td><td>443</td><td>2018-12-16T13:13:28.000Z</td></tr>
<tr><td colspan="6">Description:
The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>209.163.213.134</td><td>443</td><td>2018-12-16T13:13:28.000Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers</td></tr>
</table>

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	209.163.213.134	443	2018-12-16T13:13:28.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.76.100	443	2018-12-15T14:29:43.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	192.131.76.100	443	2018-12-15T14:29:43.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	192.131.76.100	443	2018-12-15T14:29:43.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	192.131.76.100	443	2018-12-15T14:29:43.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.76.100	443	2018-12-15T14:29:43.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	192.131.76.100	443	2018-12-15T14:29:43.000Z
Description:					

<table>
<tr><td colspan="6">There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>192.131.76.100</td><td>443</td><td>2018-12-15T14:29:43.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2016-0703</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-0703</td><td>2016-03-02</td><td>209.163.213.134</td><td>80</td><td>2018-12-11T04:15:36.000Z</td></tr>
<tr><td colspan="6">Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>209.163.213.134</td><td>80</td><td>2018-12-11T04:15:36.000Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>209.163.213.134</td><td>80</td><td>2018-12-11T04:15:36.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2015-3195</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3195</td><td>2015-12-06</td><td>209.163.213.134</td><td>80</td><td>2018-12-11T04:15:36.000Z</td></tr>
<tr><td colspan="6">Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.</td></tr>
<tr><td>CVE-2015-0232</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-0232</td><td>2015-01-27</td><td>209.163.213.134</td><td>80</td><td>2018-12-11T04:15:36.000Z</td></tr>
<tr><td colspan="6">Description:
The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.</td></tr>
<tr><td>CVE-2015-3197</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3197</td><td>2016-02-14</td><td>209.163.213.134</td><td>80</td><td>2018-12-11T04:15:36.000Z</td></tr>
<tr><td colspan="6">Description:
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.</td></tr>
</table>

CVE-2014-3670	https://nvd.nist.gov/vuln/detail/CVE-2014-3670	2014-10-29	209.163.213.134	80	2018-12-11T04:15:36.000Z
Description: The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	209.163.213.134	80	2018-12-11T04:15:36.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	209.163.213.134	80	2018-12-11T04:15:36.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	209.163.213.134	80	2018-12-11T04:15:36.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-3597	https://nvd.nist.gov/vuln/detail/CVE-2014-3597	2014-08-22	209.163.213.134	80	2018-12-11T04:15:36.000Z
Description: Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.149.172.164	443	2018-12-07T20:20:28.426Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.222.72.13	443	2018-12-07T11:12:33.427Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.92.20	443	2018-12-01T09:53:55.225Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.92.20	443	2018-12-01T09:53:55.225Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.92.20	443	2018-12-01T09:53:55.225Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.92.20	443	2018-12-01T09:53:55.225Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.92.20	443	2018-12-01T09:53:55.225Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.92.20	443	2018-12-01T09:53:55.225Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.92.20	443	2018-12-01T09:53:55.225Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.76	443	2018-12-01T05:12:05.184Z

Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.76	443	2018-12-01T05:12:05.184Z

Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.76	443	2018-12-01T05:12:05.184Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.76	443	2018-12-01T05:12:05.184Z

Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.76	443	2018-12-01T05:12:05.184Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.76	443	2018-12-01T05:12:05.184Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.76	443	2018-12-01T05:12:05.184Z

Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require

directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.132	443	2018-11-30T19:25:11.325Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.132	443	2018-11-30T19:25:11.325Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.132	443	2018-11-30T19:25:11.325Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.132	443	2018-11-30T19:25:11.325Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.132	443	2018-11-30T19:25:11.325Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.132	443	2018-11-30T19:25:11.325Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.132	443	2018-11-30T19:25:11.325Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.88	443	2018-11-30T18:54:11.321Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.88	443	2018-11-30T18:54:11.321Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.88	443	2018-11-30T18:54:11.321Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.88	443	2018-11-30T18:54:11.321Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.88	443	2018-11-30T18:54:11.321Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.88	443	2018-11-30T18:54:11.321Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a					

private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.88	443	2018-11-30T18:54:11.321Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.155	443	2018-11-17T18:30:12.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.155	443	2018-11-17T18:30:12.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.155	443	2018-11-17T18:30:12.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.155	443	2018-11-17T18:30:12.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.155	443	2018-11-17T18:30:12.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.155	443	2018-11-17T18:30:12.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.155	443	2018-11-17T18:30:12.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.155	443	2018-11-17T18:30:12.000Z

Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	63.240.88.6	443	2018-11-16T08:28:28.000Z

Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	63.240.88.6	443	2018-11-16T08:28:28.000Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	64.128.99.203	443	2018-11-15T14:09:57.000Z

Description:
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	64.128.99.203	443	2018-11-15T14:09:57.000Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	64.128.99.203	443	2018-11-15T14:09:57.000Z

Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	64.128.99.203	443	2018-11-15T14:09:57.000Z

Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before

1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.128.99.203	443	2018-11-15T14:09:57.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	64.128.99.203	443	2018-11-15T14:09:57.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	64.128.99.203	443	2018-11-15T14:09:57.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	64.128.99.203	443	2018-11-15T14:09:57.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	63.251.77.220	443	2018-11-09T13:22:52.450Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.109	443	2018-11-08T08:40:47.752Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.68	443	2018-11-06T23:51:02.464Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.60	443	2018-11-06T23:50:23.700Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.65	443	2018-11-06T23:32:23.425Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.33	443	2018-10-23T01:30:22.924Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	192.131.76.100	443	2018-10-22T11:12:21.001Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	192.131.76.100	443	2018-10-22T11:12:21.001Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	192.131.76.100	443	2018-10-22T11:12:21.001Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	192.131.76.100	443	2018-10-22T11:12:21.001Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	50.58.10.133	443	2018-10-22T09:47:25.478Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.6.220	443	2018-10-21T18:56:59.069Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works					

<table>
<tr><td colspan="6">as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2017-3736</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3736</td><td>2017-11-02</td><td>166.73.6.220</td><td>443</td><td>2018-10-21T18:56:59.069Z</td></tr>
<tr><td colspan="6">Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>166.73.6.220</td><td>443</td><td>2018-10-21T18:56:59.069Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>166.73.6.220</td><td>443</td><td>2018-10-21T18:56:59.069Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</td></tr>
<tr><td>CVE-2017-3738</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3738</td><td>2017-12-07</td><td>166.73.6.220</td><td>443</td><td>2018-10-21T18:56:59.069Z</td></tr>
<tr><td colspan="6">Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.</td></tr>
<tr><td>CVE-2015-3185</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3185</td><td>2015-07-20</td><td>166.73.6.220</td><td>443</td><td>2018-10-21T18:56:59.069Z</td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>166.73.6.220</td><td>443</td><td>2018-10-21T18:56:59.069Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
</table>

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.14.174.232	636	2018-10-11T18:31:07.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.149.172.103	443	2018-10-09T02:17:29.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	50.58.9.48	443	2018-10-09T01:28:04.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	50.58.9.181	443	2018-10-09T01:17:35.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	209.163.213.137	443	2018-10-07T10:42:39.000Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.66.20.31	443	2018-09-15T15:20:24.809Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.66.20.31	443	2018-09-15T15:20:24.809Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-	2017-11-02	208.66.20.31	443	2018-09-15T15:20:24.809Z

	3736				
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.149.172.167	443	2018-09-10T15:45:49.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.235	-	2018-09-08T23:06:23.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.237	-	2018-09-08T22:58:36.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	166.73.11.22	-	2018-09-07T12:28:01.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.213	-	2018-09-07T10:50:12.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.148	-	2018-08-18T07:58:01.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	192.131.76.23	443	2018-08-17T09:55:55.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	192.131.76.23	443	2018-08-17T09:55:55.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	192.131.76.23	443	2018-08-17T09:55:55.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.76.23	443	2018-08-17T09:55:55.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.76.23	443	2018-08-17T09:55:55.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.76.23	443	2018-08-17T09:55:55.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	192.131.76.23	443	2018-08-17T09:55:55.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.246	-	2018-08-16T20:57:24.000Z

Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.48	-	2018-08-16T19:27:59.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.235.248.231	443	2018-08-16T14:03:13.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.235.248.231	-	2018-08-16T14:03:13.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.235.248.231	443	2018-08-16T14:03:13.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.235.248.231	443	2018-08-16T14:03:13.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.235.248.231	443	2018-08-16T14:03:13.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.235.248.231	443	2018-08-16T14:03:13.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-	2016-03-02	208.235.248.231	443	2018-08-16T14:03:13.000Z

	0703				
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.235.248.231	-	2018-08-16T14:03:13.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.149.172.137	443	2018-08-16T04:41:32.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.71	443	2018-08-12T15:14:23.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-0204	https://nvd.nist.gov/vuln/detail/CVE-2015-0204	2015-01-08	209.163.213.118	-	2018-08-12T14:31:57.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	209.163.213.118	-	2018-08-12T14:31:57.000Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.118	443	2018-08-12T14:31:57.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.235.248.43	443	2018-08-11T13:02:46.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-	2017-04-17	198.167.0.133	-	2018-08-11T13:00:12.558Z

	5647				
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.248	-	2018-08-11T11:06:11.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.74.12.10	443	2018-08-11T08:57:55.511Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	64.149.172.137	-	2018-08-11T03:56:15.536Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	67.63.175.70	-	2018-08-11T03:10:42.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.11.141.38	443	2018-08-10T20:27:35.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	205.219.236.229	443	2018-08-10T06:51:35.000Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.235.248.86	-	2018-08-10T02:38:55.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vu	2014-10-14	208.235.248.122	443	2018-08-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	ln/detail/CVE-2014-3566				10T02:33:12.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	63.128.95.117	-	2018-08-09T11:59:43.000Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	166.73.12.26	-	2018-08-09T01:22:15.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-4000	https://nvd.nist.gov/vuln/detail/CVE-2015-4000	2015-05-20	64.149.172.137	-	2018-08-08T16:20:46.000Z
Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.					
CVE-2015-0204	https://nvd.nist.gov/vuln/detail/CVE-2015-0204	2015-01-08	64.149.172.137	-	2018-08-08T16:20:46.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.149.172.137	-	2018-08-08T16:20:46.000Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	63.240.88.6	-	2018-07-19T00:54:48.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	63.240.88.6	-	2018-07-19T00:54:48.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-	2015-07-20	208.11.141.155	-	2018-07-18T20:31:47.000Z

	3183				
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.155	-	2018-07-18T20:31:47.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.155	-	2018-07-18T20:31:47.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.155	-	2018-07-18T20:31:47.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.92	-	2018-07-18T10:53:59.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.92	-	2018-07-18T10:53:59.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.92	-	2018-07-18T10:53:59.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vu	2014-07-20	208.11.141.92	-	2018-07-

	ln/detail/CVE-2014-0226				18T10:53:59.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.88	-	2018-07-14T02:08:32.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.88	-	2018-07-14T02:08:32.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.88	-	2018-07-14T02:08:32.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.88	-	2018-07-14T02:08:32.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.91	-	2018-07-12T18:48:43.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.91	-	2018-07-12T18:48:43.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-	2017-07-27	208.11.141.91	-	2018-07-12T18:48:43.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	8743				
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.91	-	2018-07-12T18:48:43.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.91	-	2018-07-12T18:48:43.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.91	-	2018-07-12T18:48:43.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.207	-	2018-07-11T04:32:58.625Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	166.73.13.26	-	2018-07-10T19:11:38.897Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.129	-	2018-06-27T06:26:54.289Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	209.163.213.129	-	2018-06-27T06:26:53.920Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.76.203	-	2018-06-23T10:38:08.387Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.76.78	-	2018-06-23T10:27:43.342Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.84	-	2018-06-23T06:51:57.123Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.238	-	2018-06-23T05:37:48.985Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.237	-	2018-06-23T05:24:21.900Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.239	-	2018-06-23T05:17:58.401Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.60	-	2018-06-23T03:36:36.117Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.136	-	2018-06-23T03:25:11.211Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vu	2014-10-14	64.128.99.71	-	2018-06-

	ln/detail/CVE-2014-3566				23T03:20:57.449Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.65	-	2018-06-23T03:16:00.204Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.31.22.6	-	2018-06-22T22:29:12.320Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	198.246.154.221	-	2018-06-22T18:10:31.019Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	166.73.13.54	-	2018-06-22T02:31:21.737Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.149.172.167	-	2018-06-22T02:15:43.825Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.46.150	-	2018-06-21T01:52:19.143Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.76.202	-	2018-06-21T01:48:38.839Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	192.131.72.207	-	2018-06-20T20:06:33.945Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	69.164.81.28	-	2018-06-20T19:52:24.454Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	192.131.76.100	-	2018-06-20T16:30:45.000Z

Description:
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	192.131.76.100	-	2018-06-20T16:30:45.000Z

Description:
crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.76.100	-	2018-06-20T16:30:45.000Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.76.100	-	2018-06-20T16:30:45.000Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.76.100	-	2018-06-20T16:30:45.000Z

Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	192.131.76.100	-	2018-06-20T16:30:45.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	192.131.76.100	-	2018-06-20T16:30:45.000Z

Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	192.131.76.100	-	2018-06-20T16:30:45.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.235.248.122	-	2018-06-20T15:43:02.164Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	64.128.99.203	-	2018-06-20T14:28:05.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	64.128.99.203	-	2018-06-20T14:28:05.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	64.128.99.203	-	2018-06-20T14:28:05.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.128.99.203	-	2018-06-20T14:28:05.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	64.128.99.203	-	2018-06-20T14:28:05.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	64.128.99.203	-	2018-06-20T14:28:05.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	64.128.99.203	-	2018-06-20T14:28:05.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	64.128.99.203	-	2018-06-20T14:28:05.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.13.244	-	2018-06-20T12:53:57.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.13.244	-	2018-06-20T12:53:57.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.13.244	-	2018-06-20T12:53:57.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.13.244	-	2018-06-20T12:53:57.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.13.244	-	2018-06-20T12:53:57.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.13.244	-	2018-06-20T12:53:57.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.13.244	-	2018-06-20T12:53:57.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	64.128.99.92	-	2018-06-20T11:36:31.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	64.128.99.92	-	2018-06-20T11:36:31.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	64.128.99.92	-	2018-06-20T11:36:31.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	64.128.99.92	-	2018-06-20T11:36:31.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	64.128.99.92	-	2018-06-20T11:36:31.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-					

the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.128.99.92	-	2018-06-20T11:36:31.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	64.128.99.92	-	2018-06-20T11:36:31.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	64.128.99.92	-	2018-06-20T11:36:31.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	50.58.10.133	-	2018-06-20T07:25:52.777Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.66.20.31	-	2018-06-20T06:17:06.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.66.20.31	-	2018-06-20T06:17:06.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.66.20.31	-	2018-06-20T06:17:06.000Z

Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.118	-	2018-06-20T02:09:06.653Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	166.73.6.60	-	2018-06-19T21:41:08.252Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.11.141.38	-	2018-06-19T21:05:27.815Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	63.128.95.117	-	2018-06-19T17:51:01.888Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.6.118	-	2018-06-19T11:26:09.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.6.117	-	2018-06-19T11:25:05.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.6.117	-	2018-06-19T11:25:05.000Z
Description:					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.6.117	-	2018-06-19T11:25:05.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.92	-	2018-06-19T11:08:41.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.92	-	2018-06-19T11:08:41.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.92	-	2018-06-19T11:08:41.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.75	-	2018-06-19T11:08:30.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.75	-	2018-06-19T11:08:30.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.177	-	2018-06-19T11:04:01.000Z

Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.78	-	2018-06-19T10:55:59.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.78	-	2018-06-19T10:55:59.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.78	-	2018-06-19T10:55:59.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.78	-	2018-06-19T10:55:59.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.78	-	2018-06-19T10:55:59.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.78	-	2018-06-19T10:55:59.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3737	https://nvd.nist.gov/vu	2017-12-07	208.11.141.78	-	2018-06-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

<table>
<tr><td></td><td>ln/detail/CVE-2017-3737</td><td></td><td></td><td></td><td>19T10:55:59.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2015-3185</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3185</td><td>2015-07-20</td><td>208.11.141.155</td><td>-</td><td>2018-06-19T05:25:46.000Z</td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>208.11.141.155</td><td>-</td><td>2018-06-19T05:25:46.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2016-0703</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-0703</td><td>2016-03-02</td><td>208.11.141.155</td><td>-</td><td>2018-06-19T05:25:46.000Z</td></tr>
<tr><td colspan="6">Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.</td></tr>
<tr><td>CVE-2015-3197</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3197</td><td>2016-02-14</td><td>208.11.141.155</td><td>-</td><td>2018-06-19T05:25:46.000Z</td></tr>
<tr><td colspan="6">Description:
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.</td></tr>
<tr><td>CVE-2017-5647</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-5647</td><td>2017-04-17</td><td>198.167.0.17</td><td>-</td><td>2018-06-19T03:03:57.000Z</td></tr>
<tr><td colspan="6">Description:
A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.</td></tr>
<tr><td>CVE-2017-3738</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3738</td><td>2017-12-07</td><td>166.73.14.117</td><td>-</td><td>2018-06-19T02:47:08.000Z</td></tr>
<tr><td colspan="6">Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be</td></tr>
</table>

included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.14.117	-	2018-06-19T02:47:08.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.14.117	-	2018-06-19T02:47:08.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.129	-	2018-06-19T02:23:01.233Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	209.163.213.129	-	2018-06-19T02:23:00.878Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.130	-	2018-06-19T02:17:39.014Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	209.163.213.130	-	2018-06-19T02:17:38.652Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.138	-	2018-06-19T02:13:18.076Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.235.248.43	-	2018-06-19T01:54:47.200Z

Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.48	-	2018-06-19T01:45:22.193Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	64.128.99.68	-	2018-06-19T00:06:33.740Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	198.246.154.136	-	2018-06-18T22:50:07.203Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.170	-	2018-06-18T22:00:04.797Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	69.164.81.29	-	2018-06-18T21:09:37.575Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.149.172.137	-	2018-06-18T18:20:08.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	192.131.72.236	-	2018-06-18T16:50:16.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.72.203	-	2018-06-18T16:42:46.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers					

improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.72.203	-	2018-06-18T16:42:46.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.91	-	2018-06-18T15:45:34.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.91	-	2018-06-18T15:45:34.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.91	-	2018-06-18T15:45:34.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.91	-	2018-06-18T15:45:34.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.88	-	2018-06-18T15:37:06.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.88	-	2018-06-18T15:37:06.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.88	-	2018-06-18T15:37:06.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.88	-	2018-06-18T15:37:06.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.88	-	2018-06-18T15:37:06.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.88	-	2018-06-18T15:37:06.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.88	-	2018-06-18T15:37:06.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.88	-	2018-06-18T15:37:06.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.76	-	2018-06-18T15:37:03.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.76	-	2018-06-18T15:37:03.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.76	-	2018-06-18T15:37:03.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.76	-	2018-06-18T15:37:03.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.76	-	2018-06-18T15:37:03.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.76	-	2018-06-18T15:37:03.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.76	-	2018-06-18T15:37:03.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.196	-	2018-06-18T14:04:53.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

<table>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>208.11.141.196</td><td>-</td><td>2018-06-18T14:04:53.000Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</td></tr>
<tr><td>CVE-2015-3197</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3197</td><td>2016-02-14</td><td>208.11.141.196</td><td>-</td><td>2018-06-18T14:04:53.000Z</td></tr>
<tr><td colspan="6">Description:
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>208.11.141.196</td><td>-</td><td>2018-06-18T14:04:53.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2015-3194</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3194</td><td>2015-12-06</td><td>208.11.141.196</td><td>-</td><td>2018-06-18T14:04:53.000Z</td></tr>
<tr><td colspan="6">Description:
crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.</td></tr>
<tr><td>CVE-2016-0703</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-0703</td><td>2016-03-02</td><td>208.11.141.196</td><td>-</td><td>2018-06-18T14:04:53.000Z</td></tr>
<tr><td colspan="6">Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.</td></tr>
<tr><td>CVE-2015-3195</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3195</td><td>2015-12-06</td><td>208.11.141.196</td><td>-</td><td>2018-06-18T14:04:53.000Z</td></tr>
<tr><td colspan="6">Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.</td></tr>
<tr><td>CVE-2015-3185</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3185</td><td>2015-07-20</td><td>208.11.141.196</td><td>-</td><td>2018-06-18T14:04:53.000Z</td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2015-3195</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3195</td><td>2015-12-06</td><td>208.11.141.167</td><td>-</td><td>2018-06-18T14:03:31.000Z</td></tr>
<tr><td colspan="6">Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive</td></tr>
</table>

information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.167	-	2018-06-18T14:03:31.000Z

Description:
crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.167	-	2018-06-18T14:03:31.000Z

Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.167	-	2018-06-18T14:03:31.000Z

Description:
ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.167	-	2018-06-18T14:03:31.000Z

Description:
The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.167	-	2018-06-18T14:03:31.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.167	-	2018-06-18T14:03:31.000Z

Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	209.163.213.137	-	2018-06-18T13:13:54.691Z

Description:
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.235.248.231	-	2018-06-18T12:26:57.000Z

Description:
The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and

1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.235.248.231	-	2018-06-18T12:26:57.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.235.248.231	-	2018-06-18T12:26:57.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.235.248.231	-	2018-06-18T12:26:57.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.235.248.231	-	2018-06-18T12:26:57.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.235.248.231	-	2018-06-18T12:26:57.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	64.149.172.15	-	2018-06-18T11:44:43.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	64.149.172.15	-	2018-06-18T11:44:43.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	64.149.172.15	-	2018-06-18T11:44:43.000Z

Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.149.172.15	-	2018-06-18T11:44:43.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	64.149.172.15	-	2018-06-18T11:44:43.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	64.149.172.15	-	2018-06-18T11:44:43.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	64.149.172.15	-	2018-06-18T11:44:43.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	64.149.172.15	-	2018-06-18T11:44:43.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-0800	https://nvd.nist.gov/vuln/detail/CVE-2016-0800	2016-03-01	205.219.236.229	-	2018-06-18T11:35:59.907Z
Description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.164.210	-	2018-06-18T08:40:28.805Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-	2014-10-14	12.16.165.142	-	2018-06-18T04:22:17.241Z

	3566				
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.109	-	2018-06-18T03:42:52.313Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.16.165.87	-	2018-06-18T03:35:29.240Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-4000	https://nvd.nist.gov/vuln/detail/CVE-2015-4000	2015-05-20	12.16.165.87	-	2018-06-18T03:35:29.240Z
Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.					
CVE-2015-0204	https://nvd.nist.gov/vuln/detail/CVE-2015-0204	2015-01-08	12.16.165.87	-	2018-06-18T03:35:29.239Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.210	-	2018-06-17T20:11:19.550Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	204.95.150.200	-	2018-06-17T20:00:13.871Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-0204	https://nvd.nist.gov/vuln/detail/CVE-2015-0204	2015-01-08	204.95.150.47	-	2018-06-17T17:28:08.735Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	208.31.22.1	-	2018-06-16T23:13:47.875Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					

CVE-2014-3566	https://nvd.nist.gov/vuln/detail/CVE-2014-3566	2014-10-14	12.44.79.219	-	2018-06-16T20:01:11.921Z
Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.155	-	2018-06-13T20:31:22.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.155	-	2018-06-13T20:31:22.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.155	-	2018-06-13T20:31:22.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.155	-	2018-06-13T20:31:22.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.155	-	2018-06-13T20:31:22.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	208.11.141.155	-	2018-06-13T20:31:22.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.155	-	2018-06-13T20:31:22.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	208.11.141.155	-	2018-06-13T20:31:22.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.17	-	2018-06-13T17:40:50.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.246	-	2018-06-13T14:42:16.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.91	-	2018-06-12T14:33:32.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	208.11.141.73	-	2018-06-12T14:26:49.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	208.11.141.73	-	2018-06-12T14:26:49.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.73	-	2018-06-12T14:26:49.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.13.27	-	2018-05-20T05:35:39.000Z
Description:					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.72.203	-	2018-05-20T05:35:39.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	192.131.76.193	-	2018-05-20T05:35:39.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	192.131.72.203	-	2018-05-20T05:35:39.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.13.27	-	2018-05-20T05:35:39.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	166.73.6.118	-	2018-05-20T05:35:39.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.66.20.31	-	2018-05-20T05:35:39.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.66.20.31	-	2018-05-20T05:35:39.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a					

private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.48	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.133	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	166.73.6.118	-	2018-05-20T05:35:39.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.246	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.13.27	-	2018-05-20T05:35:39.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.6.118	-	2018-05-20T05:35:39.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.55.83	-	2018-05-20T05:35:39.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

<table>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>64.128.99.92</td><td>-</td><td>2018-05-20T05:35:39.000Z</td></tr>
<tr><td colspan="6">Description:
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>198.167.0.17</td><td>-</td><td>2018-05-20T05:35:39.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-3736</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3736</td><td>2017-11-02</td><td>166.73.13.27</td><td>-</td><td>2018-05-20T05:35:39.000Z</td></tr>
<tr><td colspan="6">Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</td></tr>
<tr><td>CVE-2015-3183</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3183</td><td>2015-07-20</td><td>192.131.76.193</td><td>-</td><td>2018-05-20T05:35:39.000Z</td></tr>
<tr><td colspan="6">Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>198.167.0.148</td><td>-</td><td>2018-05-20T05:35:39.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>192.131.55.83</td><td>-</td><td>2018-05-20T05:35:39.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vu</td><td>2014-07-20</td><td>192.131.76.100</td><td>-</td><td>2018-05-</td></tr>
</table>

	ln/detail/CVE-2014-0226				20T05:35:39.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.76.100	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.76.100	-	2018-05-20T05:35:39.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.6.118	-	2018-05-20T05:35:39.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.13.27	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.72.203	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	192.131.55.82	-	2018-05-20T05:35:39.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	166.73.6.118	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.76.193	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.72.203	-	2018-05-20T05:35:39.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	192.131.55.82	-	2018-05-20T05:35:39.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.248	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	192.131.55.82	-	2018-05-20T05:35:39.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-	2015-07-20	192.131.76.100	-	2018-05-20T05:35:39.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	3183				
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	166.73.6.118	-	2018-05-20T05:35:39.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	198.167.0.33	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	166.73.13.27	-	2018-05-20T05:35:39.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.66.20.31	-	2018-05-20T05:35:39.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	63.240.88.6	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	166.73.13.27	-	2018-05-20T05:35:39.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms					

are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	192.131.55.82	-	2018-05-20T05:35:39.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	192.131.55.83	-	2018-05-20T05:35:39.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	192.131.55.83	-	2018-05-20T05:35:39.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	192.131.76.193	-	2018-05-20T05:35:39.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	166.73.6.118	-	2018-05-20T05:35:39.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.149.172.15	-	2018-05-20T01:09:32.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.149.172.137	-	2018-05-20T01:09:32.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	64.149.172.15	-	2018-05-20T00:51:30.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	64.149.172.15	-	2018-05-20T00:51:30.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	64.149.172.15	-	2018-05-20T00:51:30.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	64.149.172.15	-	2018-05-20T00:51:30.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	64.149.172.15	-	2018-05-20T00:51:30.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	64.149.172.15	-	2018-05-20T00:51:30.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	64.149.172.15	-	2018-05-20T00:51:30.000Z
Description:					

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	64.128.99.203	-	2018-05-20T00:10:03.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	192.131.76.193	-	2018-05-19T20:01:52.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	64.128.99.203	-	2018-05-19T20:01:52.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	192.131.72.203	-	2018-05-19T20:01:52.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	192.131.72.203	-	2018-05-19T20:01:52.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	64.128.99.203	-	2018-05-19T20:01:52.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	64.128.99.203	-	2018-05-19T20:01:52.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.92	-	2018-05-19T20:01:52.000Z

Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3197	https://nvd.nist.gov/vuln/detail/CVE-2015-3197	2016-02-14	192.131.72.203	-	2018-05-19T20:01:52.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2016-0703	https://nvd.nist.gov/vuln/detail/CVE-2016-0703	2016-03-02	192.131.76.193	-	2018-05-19T20:01:52.000Z
Description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	192.131.76.193	-	2018-05-19T20:01:52.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	64.128.99.203	-	2018-05-19T20:01:52.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.92	-	2018-05-19T20:01:52.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3194	https://nvd.nist.gov/vuln/detail/CVE-2015-3194	2015-12-06	192.131.72.203	-	2018-05-19T20:01:52.000Z
Description: crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.92	-	2018-05-19T20:01:52.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3197	https://nvd.nist.gov/vu	2016-02-14	64.128.99.203	-	2018-05-

	ln/detail/CVE-2015-3197				19T20:01:52.000Z
Description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.92	-	2018-05-19T20:01:52.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	64.128.99.203	-	2018-05-19T20:01:52.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	192.131.76.193	-	2018-05-19T20:01:52.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2015-3195	https://nvd.nist.gov/vuln/detail/CVE-2015-3195	2015-12-06	64.128.99.203	-	2018-05-19T20:01:52.000Z
Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.17	-	2018-05-19T19:58:31.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.48	-	2018-05-19T19:58:31.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.248	-	2018-05-19T19:58:31.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.133	-	2018-05-19T19:58:31.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.33	-	2018-05-19T19:58:31.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	192.131.72.236	-	2018-05-19T19:58:31.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.148	-	2018-05-19T19:58:31.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2017-5647	https://nvd.nist.gov/vuln/detail/CVE-2017-5647	2017-04-17	198.167.0.246	-	2018-05-19T19:58:31.000Z
Description: A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.64	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.76	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					

<table>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>208.11.141.76</td><td>-</td><td>2018-05-19T12:44:21.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2017-3736</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3736</td><td>2017-11-02</td><td>208.11.141.204</td><td>-</td><td>2018-05-19T12:44:21.000Z</td></tr>
<tr><td colspan="6">Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>208.11.141.76</td><td>-</td><td>2018-05-19T12:44:21.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2017-3737</td><td>https://nvd.nist.gov/vuln/detail/CVE-2017-3737</td><td>2017-12-07</td><td>208.11.141.177</td><td>-</td><td>2018-05-19T12:44:21.000Z</td></tr>
<tr><td colspan="6">Description:
OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</td></tr>
<tr><td>CVE-2016-8743</td><td>https://nvd.nist.gov/vuln/detail/CVE-2016-8743</td><td>2017-07-27</td><td>208.11.141.132</td><td>-</td><td>2018-05-19T12:44:21.000Z</td></tr>
<tr><td colspan="6">Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</td></tr>
<tr><td>CVE-2015-3185</td><td>https://nvd.nist.gov/vuln/detail/CVE-2015-3185</td><td>2015-07-20</td><td>208.11.141.78</td><td>-</td><td>2018-05-19T12:44:21.000Z</td></tr>
<tr><td colspan="6">Description:
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</td></tr>
<tr><td>CVE-2014-0226</td><td>https://nvd.nist.gov/vuln/detail/CVE-2014-0226</td><td>2014-07-20</td><td>208.11.141.88</td><td>-</td><td>2018-05-19T12:44:21.000Z</td></tr>
</table>

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.192	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.167	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.75	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.196	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.192	-	2018-05-19T12:44:21.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.132	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.177	-	2018-05-19T12:44:21.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-					

2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.91	-	2018-05-19T12:44:21.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.177	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.91	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.196	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.155	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.177	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.132	-	2018-05-19T12:44:21.000Z
Description:					

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.92	-	2018-05-19T12:44:21.000Z

Description:
There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.204	-	2018-05-19T12:44:21.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.177	-	2018-05-19T12:44:21.000Z

Description:
The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.177	-	2018-05-19T12:44:21.000Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.204	-	2018-05-19T12:44:21.000Z

Description:
There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.91	-	2018-05-19T12:44:21.000Z

Description:
Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.155	-	2018-05-19T12:44:21.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.75	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.75	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.155	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.204	-	2018-05-19T12:44:21.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.196	-	2018-05-19T12:44:21.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.76	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.192	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					

CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.73	-	2018-05-19T12:44:21.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.75	-	2018-05-19T12:44:21.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.204	-	2018-05-19T12:44:21.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.177	-	2018-05-19T12:44:21.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.78	-	2018-05-19T12:44:21.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.92	-	2018-05-19T12:44:21.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-	2017-07-27	208.11.141.64	-	2018-05-19T12:44:21.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	8743				
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.78	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3737	https://nvd.nist.gov/vuln/detail/CVE-2017-3737	2017-12-07	208.11.141.91	-	2018-05-19T12:44:21.000Z
Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.					
CVE-2017-3736	https://nvd.nist.gov/vuln/detail/CVE-2017-3736	2017-11-02	208.11.141.76	-	2018-05-19T12:44:21.000Z
Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.167	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.73	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.92	-	2018-05-19T12:44:21.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on					

TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2016-8743	https://nvd.nist.gov/vuln/detail/CVE-2016-8743	2017-07-27	208.11.141.88	-	2018-05-19T12:44:21.000Z
Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.88	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2017-3738	https://nvd.nist.gov/vuln/detail/CVE-2017-3738	2017-12-07	208.11.141.76	-	2018-05-19T12:44:21.000Z
Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.204	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.88	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.91	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.132	-	2018-05-19T12:44:21.000Z
Description:					

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.167	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.196	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.76	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.73	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-0226	2014-07-20	208.11.141.155	-	2018-05-19T12:44:21.000Z
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.64	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2015-3183	https://nvd.nist.gov/vuln/detail/CVE-2015-3183	2015-07-20	208.11.141.78	-	2018-05-19T12:44:21.000Z
Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.					
CVE-2014-0226	https://nvd.nist.gov/vuln/detail/CVE-2014-	2014-07-20	208.11.141.192	-	2018-05-19T12:44:21.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	0226				
Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.					
CVE-2015-3185	https://nvd.nist.gov/vuln/detail/CVE-2015-3185	2015-07-20	208.11.141.204	-	2018-05-19T12:44:21.000Z
Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.					

RECOMMENDATION

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the BugTraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

ABOUT THIS ISSUE

Based on scan data, the company had medium severity CVE vulnerability that was open longer than 60 days after the CVE was published. Medium severity CVEs are those with a documented CVSS severity between 4.0 and 6.9. It is best practice to mitigate or patch medium severity vulnerabilities within 60 days. Details on each vulnerability are listed in the table below.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

B 89 ENDPOINT SECURITY

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The Endpoint Security Module tracks identification points that are extracted from metadata related to the operating system, web browser, and related active plugins. The information gathered allows companies to identify outdated versions of these data points which can lead to client-side exploitation attacks.

!!! HIGH SEVERITY

There are no High Risk Issues to detect for Endpoint Security

!! MEDIUM SEVERITY

Outdated Web Browser Observed	22
Outdated Operating System Observed	0

! LOW SEVERITY

There are no Low Risk Issues to detect for Endpoint Security

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Endpoint Security

i INFORMATIONAL

Multiple Browsers Detected	0

ENDPOINT SECURITY > ISSUE DETAIL

!! Outdated Web Browser Observed

An outdated web browser connected to a web server.

-0.4 SCORE IMPACT

22 findings

SOURCE IP	PRODUCT MANUFACTURER	PRODUCT NAME	PRODUCT TYPE	PRODUCT VERSION	PRODUCT LATEST VERSION	LAST SEEN
12.180.126.100	Google	Chrome	browser	61.0.3163.79	69.0.3497.100	2019-01-31T02:00:00.000Z
208.66.22.2	Google	Chrome	browser	65.0.3325.162	69.0.3497.100	2019-01-30T23:00:00.000Z
204.95.150.205	Google	Chrome	browser	65.0.3325.181	69.0.3497.100	2019-01-30T20:08:39.000Z
65.202.81.138	Google	Chrome	browser	66.0.3359.139	69.0.3497.100	2019-01-30T17:15:50.000Z
204.95.150.205	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01-30T16:57:45.000Z
103.1.128.11	Google	Chrome	browser	44.0.2403.89	69.0.3497.100	2019-01-30T07:38:29.000Z
12.27.169.18	Apple	Safari	browser	9.1.2	12.0	2019-01-29T20:33:50.000Z

12.16.164.205	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01-29T15:42:21.000Z
208.66.22.2	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01-29T14:32:30.000Z
103.1.128.11	Google	Chrome	browser	51.0.2704.84	69.0.3497.100	2019-01-29T08:23:15.000Z
166.73.28.27	Google	Chrome	browser	42.0.2311.152	69.0.3497.100	2019-01-28T20:34:50.000Z
166.73.228.150	Google	Chrome	browser	43.0.2357.130	69.0.3497.100	2019-01-28T18:33:26.000Z
103.1.128.11	Google	Chrome	browser	33.0.1736.2	69.0.3497.100	2019-01-28T10:54:48.000Z
12.180.126.100	Google	Chrome	browser	64.0.3282.119	69.0.3497.100	2019-01-27T22:57:46.000Z
12.175.11.5	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01-25T18:25:37.000Z
12.2.10.242	Google	Chrome	browser	65.0.3325.162	69.0.3497.100	2019-01-22T16:33:05.000Z
12.2.10.242	Microsoft	Edge	browser	14.14393	42.17134.1.0	2019-01-22T16:15:19.000Z
103.1.131.254	Google	Chrome	browser	62.0.3202.94	69.0.3497.100	2019-01-11T14:00:00.000Z
64.149.173.195	Mozilla	Firefox	browser	56.0	62.0.2	2019-01-09T17:18:17.000Z
208.66.22.2	Mozilla	Firefox	browser	56.0	62.0.2	2019-01-06T12:59:18.000Z
65.206.30.70	Apple	Safari	browser	9.1.1	12.0	2019-01-03T14:00:48.000Z
166.73.129.157	Google	Chrome	browser	60.0.3112.113	69.0.3497.100	2019-01-02T21:49:19.000Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

RECOMMENDATION

Update the web browsers in question. Enable automatic updates if available from your web browser vendor and permitted in your environment.

ABOUT THIS ISSUE

The web is constantly evolving, using different languages, protocols, and file formats over time. Web browsers regularly release new versions, on time scales as short as every six weeks. These new versions frequently contain security and stability fixes. When a web browser connects to a web server, it informs the server its platform and version information. This information assists the server in providing appropriate content. The information can also be recorded and aggregated to determine what platforms and browser versions are being used by hosts at various places on the Internet. Using such a data set, it was found that an outdated web browser was in use as described in the table below. Note that a single external IP address, such as those in the table below, may correspond to any number of internal hosts. For example, a company firewall or NAT gateway with a single external IP will appear to be the source of an entire network full of corporate desktops.

A 100 IP REPUTATION

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The IP Reputation and Malware Exposure module makes use of the SecurityScorecard sinkhole infrastructure as well as a blend of OSINT malware feeds, and third party threat intelligence data sharing partnerships. The SecurityScorecard sinkhole system ingests millions of malware signals from commandeered Command and Control (C2) infrastructures globally from all over the world. The incoming data is processed and attributed to corporate enterprises. The quantity and duration of malware infections are used as the determining factor for calculating is module the Malware Exposure Key Threat Indicator.

!!! HIGH SEVERITY

Malware Events, Last Day	0

!! MEDIUM SEVERITY

P2P Activities	0
Attack Detected	0
Malware Events, Last Month	0

! LOW SEVERITY

Malware Events, Last Year	2

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for IP Reputation

i INFORMATIONAL

Tor Exit Nodes	0
Unsolicited Commercial Email	0

IP REPUTATION > ISSUE DETAIL

! Malware Events, Last Year

Communications indicative of malware infections were observed over the last 365 days.

2 findings

MALWARE TYPE	MALWARE FAMILY	MALWARE DETECTION METHODS	SOURCE IP	FIRST SEEN	LAST SEEN
bot	azorult	honeynet	103.1.130.48	2018-06-06T00:00:00.000Z	2018-06-06T00:00:00.000Z
bot	quant	honeynet	12.179.188.5	2018-03-26T00:00:00.000Z	2018-03-27T00:00:00.000Z

RECOMMENDATION

Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.

ABOUT THIS ISSUE

After a device has been infected by malware, it often communicates with a command and control (C&C) service on the internet. This service allows the malware to register its infected device and receive instructions from the malware's authors. These instructions could cause the device to delete or encrypt its datastores, participate in distributed denial-of-service (DDoS) attacks, or perform any variety of malicious actions.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

F 58 APPLICATION SECURITY

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The Web Application Vulnerability module uses incoming threat intelligence from known exploitable conditions identified via: whitehat CVE databases, blackhat exploit databases, and sensitive findings indexed by major search engines. The module ingests data from multiple public data sets, third party feeds, and an internal proprietary indexing and aggregation engine.

The score determines the likelihood of an upcoming web application breach, and checks for any existing defacement code. Presence of vulnerable applications, outdated versions, and active defacements are used to calculate the overall grade.

!!! HIGH SEVERITY	
Site does not enforce HTTPS	70
High Severity Content Management System vulnerabilities identified	0

!! MEDIUM SEVERITY	
Website does not implement X-XSS-Protection Best Practices	138
Website does not implement X-Frame-Options Best Practices	143
Redirect Chain Contains HTTP	4
Insecure HTTPS Redirect Pattern	6
Website Does Not Implement HSTS Best Practices	85
Medium Severity Content Management System vulnerabilities identified	0

! LOW SEVERITY	
Session Cookie Missing 'HttpOnly' Attribute	2
Website does not implement X-Content-Type-Options Best Practices	138
Cookie Missing 'Secure' Attribute	0
Low Severity Content Management System vulnerabilities identified	0

✓ POSITIVE SIGNALS	
Web Application Firewall (WAF) Detected	6
Domain Uses HSTS Preloading	0

i INFORMATIONAL	
Unsafe Implementation Of Subresource Integrity	7
Content Security Policy Contains Broad Directives	1
Content Security Policy Contains 'unsafe-*' Directive	9
Content Security Policy (CSP) Missing	145
Object Storage Bucket with Risky ACL	0
Website Hosted on Object Storage	0
Website References Object Storage	0

APPLICATION SECURITY > ISSUE DETAIL

!! Website does not implement X-XSS-Protection Best Practices

Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks.

-0.9 SCORE IMPACT

138 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
x_xss_protection_missing	https://staging.fiserv-ecomhosting.com/	https://staging.fiserv-ecomhosting.com/	n/a	Header missing	2019-01-29T09:11:43.731Z
x_xss_protection_missing	http://staging.fiserv-ecomhosting.com/	http://staging.fiserv-ecomhosting.com/	n/a	Header missing	2019-01-29T09:11:43.673Z
x_xss_protection_missing	http://www.fiservsw.com/	http://www.fiservsw.com/	n/a	Header missing	2019-01-29T09:11:42.823Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_xss_protection_missing	https://mail.fiservlendingsolutions.com/	https://mail.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:11:17.099Z
x_xss_protection_missing	http://fiservcreditservices.com/	http://fiservcreditservices.com/	n/a	Header missing	2019-01-29T09:11:15.569Z
x_xss_protection_missing	https://webmail.fiserv.net/	https://webmail.fiserv.net/	n/a	Header missing	2019-01-29T09:11:13.849Z
x_xss_protection_missing	http://fiservsw.com/	http://fiservsw.com/	n/a	Header missing	2019-01-29T09:11:05.384Z
x_xss_protection_missing	https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3a%2f%2flogin.microsoftonline.com%2fte%2ffiservservicepoint.onmicrosoft.com%2fb2c_1a_prod_sn_signin%2fsamlp%2fsso%2flogin%3fsamlrequest%3dlvlbbptaep0vthdgoxfjvsyssvxvupki2o2hf2sdg7mszjcdhsr%252fx8akts%252bwep15896bn7ni3drxq7lopeedphfaznttamr17qsis6his2gfugfwrld77o5wxyfursvhbdxcy5jboko4iesuabsh25scfj7cpuljuzzvgfzmapubn1s%252b0ktquboi7lt9gqak4w0hawb1ypr3rqatwaaxhswmyhhwbmeadtctzpwtgxqb4qd2qt3em2ouhxnl5zhxyoaebsnxwtzkpjo%252f8l6rlwbkihwvrhmet9umyn%252b%252fwzz6uutfnxyvchlheqrf4ssyizfy%252buqxquqa5fwzmx5s4ww3tjj3sen2gl0qyhklvoz8odnirewrkjk4sulfwsvncg8mlgzpl%252fn%252bpinyft8ccj%252f%252fst9mbl0pwd4p6p%252bk%252bhdynmiemmv6nd1btbbt5xe47ei%252f312sl0uvws8cs1yrrte7bu61kd68rk7pzwnbu48yh5s02l32mfzm6vctvlxjwuwanqjxs%252bq%252fd77%252baw%253d%253d%26relaystate%3dhttps%253a%252f%252ffiserv.service-now.com%252fnavpage.do	http://my.carreker.com/	http://my.carreker.com/, 302, https://c3.fiserv.com/, 302, https://servicepoint.fiservapps.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3A%2F%2Flogin.microsoftonline.com%2Fte%2Ffiservservicepoint.onmicrosoft.com%2FB2C_1A_Prod_sn_signin%2Fsamlp%2Fsso%2Flogin%3FSAMLRequest%3DlVLBbptAEP0VtHdgoXFjVsYSsVXVUpKi2O2hF2sDg7MSzJCdhSR%252FX8AkTS%252BWep15896bN7Ni3dRxq7LOPeEDPHfAznttamR17qSis6hIs2GFugFWrlD77O5WxYFUrSVHBdXCy5jBOkO4IeSuAbsH25sCfj7cpuLJuZZVGFZmAPUBn1s%252B0ktQUBOi7lt9gqAk4W0HAwb1yPR3rqaTwaAxhSWmyhHWBmEadTCTzpwtGXQB4Qd2Qt3Em2OUHXNL5ZHxyOaEBsNxwTZkpjO%252F8L6RLWBKIhWVrhmEt9umYn%252B%252FWZZ6UUTFNXyVchlHEqrF4ssyiZfy%252BuqxquQA5Fwzmx5S4Ww3TjJ3sEN2Gl0qYhklvoz8ODnIREWRkjK4SuLfwsvnCG8MlgZPl%252FN%252BPINYfT8ccj%252F%252FsT9MBL0pwd4P6P%252BK%252BhdYnmIemMV6Nd1bTbbt5xe47Ei%252F312sL0uvws8Cs1yrRte7bU61Kd68rK7pZWNBu48Yh5s02l32MFZM6VcTVLXjWuwAnQjXs%252Bq%25	Header missing	2019-01-29T09:11:00.692Z

			2FD77%252BAw%253D%253D%26RelayState%3Dhttps%253A%252F%252Ffiserv.service-now.com%252Fnavpage.do		
x_xss_protection_missing	https://search.carreker.com/	https://search.carreker.com/	n/a	Header missing	2019-01-29T09:10:57.094Z
x_xss_protection_missing	http://search.carreker.com/	http://search.carreker.com/	n/a	Header missing	2019-01-29T09:10:57.065Z
x_xss_protection_missing	https://careers.carreker.com/	https://careers.carreker.com/	n/a	Header missing	2019-01-29T09:10:56.934Z
x_xss_protection_missing	https://mail.billmatrix.com/	https://mail.billmatrix.com/	n/a	Header missing	2019-01-29T09:10:56.928Z
x_xss_protection_missing	http://careers.carreker.com/	http://careers.carreker.com/	n/a	Header missing	2019-01-29T09:10:56.855Z
x_xss_protection_missing	https://support.fiservatlanta.net/	http://support.fiservatlanta.net/	http://support.fiservatlanta.net/, 302, https://support.fiservatlanta.net/	Header missing	2019-01-29T09:10:54.014Z
x_xss_protection_missing	https://fiservwebsolutions.com/	https://fiservwebsolutions.com/	n/a	Header missing	2019-01-29T09:10:53.876Z
x_xss_protection_missing	https://alpha.hepsiian.com/	https://alpha.hepsiian.com/	n/a	Header missing	2019-01-29T09:10:53.348Z
x_xss_protection_missing	https://images.hepsiian.com/	https://images.hepsiian.com/	n/a	Header missing	2019-01-29T09:10:52.534Z
x_xss_protection_missing	https://fiservlendingsolutions.com/	https://fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.983Z
x_xss_protection_missing	http://fiservlendingsolutions.com/	http://fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.913Z
x_xss_protection_missing	https://fiservipvpn.com/	https://fiservipvpn.com/	n/a	Header missing	2019-01-29T09:10:50.584Z
x_xss_protection_missing	http://demo.billmatrix.com/	http://demo.billmatrix.com/	n/a	Header missing	2019-01-29T09:10:50.447Z
x_xss_protection_missing	https://www.fiservlendingsolutions.com/	https://www.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.369Z
x_xss_protection_missing	http://mail.fiservlendingsolutions.com/	http://mail.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.349Z
x_xss_protection_missing	http://www.fiservlendingsolutions.com/	http://www.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.285Z
x_xss_protection_missing	https://fiservcws.com/	https://fiservcws.com/	n/a	Header missing	2019-01-29T09:10:50.069Z
x_xss_protection_missing	https://www.careers.fiserv.com/	https://careers.fiserv.com/	https://careers.fiserv.com/, 301, http://www.careers.fiserv.com, 301,	Header missing	2019-01-29T09:09:27.681Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

			https://www.careers.fiserv.com/		
x_xss_protection_missing	https://alabama.fiservls.com/	https://alabama.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.824Z
x_xss_protection_missing	http://alabama.fiservls.com/	http://alabama.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.763Z
x_xss_protection_missing	https://en.fiservls.com/	https://en.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.760Z
x_xss_protection_missing	https://blog.fiservls.com/	https://blog.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.759Z
x_xss_protection_missing	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.742Z
x_xss_protection_missing	https://shop.fiservls.com/	https://shop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.731Z
x_xss_protection_missing	https://bg.fiservls.com/	https://bg.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.726Z
x_xss_protection_missing	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.715Z
x_xss_protection_missing	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.691Z
x_xss_protection_missing	http://en.fiservls.com/	http://en.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.691Z
x_xss_protection_missing	http://blog.fiservls.com/	http://blog.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.677Z
x_xss_protection_missing	http://shop.fiservls.com/	http://shop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.662Z
x_xss_protection_missing	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.662Z
x_xss_protection_missing	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.646Z
x_xss_protection_missing	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.968Z
x_xss_protection_missing	https://in.fiservls.com/	https://in.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.961Z
x_xss_protection_missing	https://ww.fiservls.com/	https://ww.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.955Z
x_xss_protection_missing	https://backend.fiservls.com/	https://backend.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z
x_xss_protection_missing	https://espanol.fiservls.com/	https://espanol.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z
x_xss_protection_missing	https://chat.fiservls.com/	https://chat.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z
x_xss_protection_missing	https://arizona.fiservls.com/	https://arizona.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.918Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_xss_protection_missing	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_xss_protection_missing	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_xss_protection_missing	http://download.fiservls.com/	http://download.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_xss_protection_missing	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_xss_protection_missing	http://backend.fiservls.com/	http://backend.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.878Z
x_xss_protection_missing	http://in.fiservls.com/	http://in.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.878Z
x_xss_protection_missing	http://espanol.fiservls.com/	http://espanol.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.863Z
x_xss_protection_missing	http://forums.fiservls.com/	http://forums.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.853Z
x_xss_protection_missing	http://arizona.fiservls.com/	http://arizona.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.849Z
x_xss_protection_missing	http://chat.fiservls.com/	http://chat.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.849Z
x_xss_protection_missing	https://14.fiservls.com/	https://14.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.091Z
x_xss_protection_missing	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.089Z
x_xss_protection_missing	https://sadmin.fiservls.com/	https://sadmin.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.085Z
x_xss_protection_missing	https://boston.fiservls.com/	https://boston.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.083Z
x_xss_protection_missing	https://developer.fiservls.com/	https://developer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.073Z
x_xss_protection_missing	https://act.fiservls.com/	https://act.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.070Z
x_xss_protection_missing	https://arlington.fiservls.com/	https://arlington.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.063Z
x_xss_protection_missing	https://client.fiservls.com/	https://client.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.063Z
x_xss_protection_missing	https://ftp.fiservls.com/	https://ftp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.047Z
x_xss_protection_missing	http://mobile.fiservls.com/	http://mobile.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.017Z
x_xss_protection_missing	http://14.fiservls.com/	http://14.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.016Z
x_xss_protection_mis	http://boston.fiservls.c	http://boston.fiservls.c	n/a	Header missing	2019-01-

sing	om/	om/			22T07:04:14.015Z
x_xss_protection_missing	http://sadmin.fiservls.com/	http://sadmin.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.014Z
x_xss_protection_missing	http://developer.fiservls.com/	http://developer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.993Z
x_xss_protection_missing	http://act.fiservls.com/	http://act.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.993Z
x_xss_protection_missing	http://client.fiservls.com/	http://client.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.990Z
x_xss_protection_missing	http://backup.fiservls.com/	http://backup.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.984Z
x_xss_protection_missing	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.780Z
x_xss_protection_missing	https://blackberry.fiservls.com/	https://blackberry.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.296Z
x_xss_protection_missing	https://citrix.fiservls.com/	https://citrix.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.214Z
x_xss_protection_missing	https://arkansas.fiservls.com/	https://arkansas.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.209Z
x_xss_protection_missing	https://biz.fiservls.com/	https://biz.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.207Z
x_xss_protection_missing	http://citrix.fiservls.com/	http://citrix.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_xss_protection_missing	http://blackberry.fiservls.com/	http://blackberry.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_xss_protection_missing	http://arkansas.fiservls.com/	http://arkansas.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_xss_protection_missing	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_xss_protection_missing	https://survey.fiservls.com/	https://survey.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.891Z
x_xss_protection_missing	https://demo.fiservls.com/	https://demo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.891Z
x_xss_protection_missing	https://au.fiservls.com/	https://au.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.849Z
x_xss_protection_missing	http://survey.fiservls.com/	http://survey.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.815Z
x_xss_protection_missing	http://demo.fiservls.com/	http://demo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.815Z
x_xss_protection_missing	http://arlington.fiservls.com/	http://arlington.fiservls.com/	n/a	Header missing	2019-01-22T07:04:05.405Z
x_xss_protection_missing	https://fiservsupport.com/	http://www.fiservsupport.com/	http://www.fiservsupport.com/, 302,	Header missing	2019-01-22T07:04:04.073Z

			http://fiservsupport.com/, 302, https://fiservsupport.com/		
x_xss_protection_missing	http://fiservdox.com/	http://fiservdox.com/	n/a	Header missing	2019-01-22T07:04:03.821Z
x_xss_protection_missing	https://team.fiservls.com/	https://team.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.075Z
x_xss_protection_missing	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.053Z
x_xss_protection_missing	http://mail.fiservls.com/	http://mail.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.030Z
x_xss_protection_missing	http://team.fiservls.com/	http://team.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.013Z
x_xss_protection_missing	https://ns1.fiservls.com/	https://ns1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.005Z
x_xss_protection_missing	https://131.fiservls.com/	https://131.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.976Z
x_xss_protection_missing	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.968Z
x_xss_protection_missing	https://forums.fiservls.com/	https://forums.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.940Z
x_xss_protection_missing	http://pop.fiservls.com/	http://pop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.920Z
x_xss_protection_missing	https://corp.fiservls.com/	https://corp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.904Z
x_xss_protection_missing	http://131.fiservls.com/	http://131.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.897Z
x_xss_protection_missing	https://apps.fiservls.com/	https://apps.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.857Z
x_xss_protection_missing	https://atlanta.fiservls.com/	https://atlanta.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.851Z
x_xss_protection_missing	http://corp.fiservls.com/	http://corp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.819Z
x_xss_protection_missing	http://apps.fiservls.com/	http://apps.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.789Z
x_xss_protection_missing	https://customer.fiservls.com/	https://customer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.784Z
x_xss_protection_missing	https://intranet1.fiservls.com/	https://intranet1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.756Z
x_xss_protection_missing	http://atlanta.fiservls.com/	http://atlanta.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.748Z
x_xss_protection_missing	https://18.fiservls.com/	https://18.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.716Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_xss_protection_missing	http://customer.fiservls.com/	http://customer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.710Z
x_xss_protection_missing	https://administrador.fiservls.com/	https://administrador.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.681Z
x_xss_protection_missing	http://intranet1.fiservls.com/	http://intranet1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.673Z
x_xss_protection_missing	http://18.fiservls.com/	http://18.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.638Z
x_xss_protection_missing	http://administrador.fiservls.com/	http://administrador.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.606Z
x_xss_protection_missing	https://backup.fiservls.com/	https://backup.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.590Z
x_xss_protection_missing	https://apollo.fiservls.com/	https://apollo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.577Z
x_xss_protection_missing	https://manage.fiservls.com/	https://manage.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.496Z
x_xss_protection_missing	http://apollo.fiservls.com/	http://apollo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.487Z
x_xss_protection_missing	https://support.fiservls.com/	https://support.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.457Z
x_xss_protection_missing	http://manage.fiservls.com/	http://manage.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.415Z
x_xss_protection_missing	http://support.fiservls.com/	http://support.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.382Z
x_xss_protection_missing	http://au.fiservls.com/	http://au.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.382Z
x_xss_protection_missing	https://email.fiservls.com/	https://email.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.113Z
x_xss_protection_missing	https://ad.fiservls.com/	https://ad.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.039Z
x_xss_protection_missing	http://email.fiservls.com/	http://email.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.030Z
x_xss_protection_missing	https://download.fiservls.com/	https://download.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.000Z
x_xss_protection_missing	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.957Z
x_xss_protection_missing	https://am.fiservls.com/	https://am.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.913Z
x_xss_protection_missing	http://am.fiservls.com/	http://am.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.824Z
x_xss_protection_missing	https://california.fiservls.com/	https://california.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.632Z
x_xss_protection_mis	https://antivirus.fiservl	https://antivirus.fiservl	n/a	Header missing	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

sing	s.com/	s.com/			22T07:04:01.624Z
x_xss_protection_missing	https://ajax.fiservls.com/	https://ajax.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.621Z
x_xss_protection_missing	https://mail.fiservls.com/	https://mail.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.617Z
x_xss_protection_missing	https://pop.fiservls.com/	https://pop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.617Z
x_xss_protection_missing	http://ajax.fiservls.com/	http://ajax.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z
x_xss_protection_missing	http://california.fiservls.com/	http://california.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z
x_xss_protection_missing	http://antivirus.fiservls.com/	http://antivirus.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z

RECOMMENDATION

Add the following header to responses from this website: 'X-XSS-Protection: 1; mode=block'

ABOUT THIS ISSUE

The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when websites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP. Without these protections, an attacker can send their victims malicious URLs that inject code into the website

APPLICATION SECURITY > ISSUE DETAIL

Website does not implement X-Content-Type-Options Best Practices

-0.3 SCORE IMPACT

Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript.

138 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
x_content_type_options_missing	https://staging.fiserv-ecomhosting.com/	https://staging.fiserv-ecomhosting.com/	n/a	Header missing	2019-01-29T09:11:43.731Z
x_content_type_options_missing	http://staging.fiserv-ecomhosting.com/	http://staging.fiserv-ecomhosting.com/	n/a	Header missing	2019-01-29T09:11:43.673Z
x_content_type_options_missing	http://www.fiservsw.com/	http://www.fiservsw.com/	n/a	Header missing	2019-01-29T09:11:42.823Z
x_content_type_optio	https://mail.fiservlendi	https://mail.fiservlendi	n/a	Header missing	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

ns_missing	ngsolutions.com/	ngsolutions.com/			29T09:11:17.099Z
x_content_type_options_missing	http://fiservcreditservices.com/	http://fiservcreditservices.com/	n/a	Header missing	2019-01-29T09:11:15.569Z
x_content_type_options_missing	https://webmail.fiserv.net/	https://webmail.fiserv.net/	n/a	Header missing	2019-01-29T09:11:13.849Z
x_content_type_options_missing	http://fiservsw.com/	http://fiservsw.com/	n/a	Header missing	2019-01-29T09:11:05.384Z
x_content_type_options_missing	https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3a%2f%2flogin.microsoftonline.com%2fte%2ffiservservicepoint.onmicrosoft.com%2fb2c_1a_prod_sn_signin%2fsamlp%2fsso%2flogin%3fsamlrequest%3dlvlbbptaep0vthdgoxfjvsyssvxvupki2o2hf2sdg7mszjcdhsr%252fx8akts%252bwep15896bn7ni3drxq7lopeedphfaznttamr17qsis6his2gfugfwrld77o5wxyfursvhbdxcy5jboko4iesuabsh25scfj7cpuljuzzvgfzmapubn1s%252b0ktquboi7lt9gqak4w0hawb1ypr3rqatwaaxhswmyhhwbmeadtctzpwtgxqb4qd2qt3em2ouhxnl5zhxyoaebsnxwtzkpjo%252f8l6rlwbkihwvrhmet9umyn%252b%252fwzz6uutfnxyvchlheqrf4ssyizfy%252buqxquqa5fwzmx5s4ww3tjj3sen2gl0qyhklvoz8odnirewrkjk4sulfwsvncg8mlgzpl%252fn%252bpinyft8ccj%252f%252fst9mbl0pwd4p6p%252bk%252bhdynmiemmv6nd1btbbt5xe47ei%252f312sl0uvws8cs1yrrte7bu61kd68rk7pzwnbu48yh5s02l32mfzm6vctvlxjwuwanqjxs%252bq%252fd77%252baw%253d%253d%26relaystate%3dhttps%253a%252f%252ffiserv.service-now.com%252fnavpage.do	http://my.carreker.com/	http://my.carreker.com/, 302, https://c3.fiserv.com/, 302, https://servicepoint.fiservapps.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3A%2F%2Flogin.microsoftonline.com%2Fte%2Ffiservservicepoint.onmicrosoft.com%2FB2C_1A_Prod_sn_signin%2Fsamlp%2Fsso%2Flogin%3FSAMLRequest%3DlVLBbptAEP0VtHdgoXFjVsYSsVXVUpKi2O2hF2sDg7MSzJCdhSR%252FX8AkTS%252BWep15896bN7Ni3dRxq7LOPeEDPHfAznttamR17qSis6hIs2GFugFWrlD77O5WxYFUrSVHBdXCy5jBOkO4IeSuAbsH25sCfj7cpuLJuZZVGFZmAPUBn1s%252B0ktQUBOi7lt9gqAk4W0HAwb1yPR3rqaTwaAxhSWmyhHWBmEadTCTzpwtGXQB4Qd2Qt3Em2OUHXNL5ZHxyOaEBsNxwTZkpjO%252F8L6RLWBKIhWVrhmEt9umYn%252B%252FWZZ6UUTFNXyVchlHEqrF4ssyiZfy%252BuqxquQA5Fwzmx5S4Ww3TjJ3sEN2Gl0qYhklvoz8ODnIREWRkjK4SuLfwsvnCG8MlgZPl%252FN%252BPlNYfT8ccj%252F%252FsT9MBL0pwd4P6P%252BK%252BhdYnmlemMV6Nd1bTbbt5xe47Ei%252F312sL0uvws8Cs1yrRte7bU61Kd68rK7pZWNBu48Yh5s02l32MFZM6VcTVLXjWuwAnQjXs%252Bq%252FD77%252BAw%253	Header missing	2019-01-29T09:11:00.692Z

			D%253D%26RelayState%3Dhttps%253A%252F%252Ffiserv.service-now.com%252Fnavpage.do		
x_content_type_options_missing	https://search.carreker.com/	https://search.carreker.com/	n/a	Header missing	2019-01-29T09:10:57.094Z
x_content_type_options_missing	http://search.carreker.com/	http://search.carreker.com/	n/a	Header missing	2019-01-29T09:10:57.065Z
x_content_type_options_missing	https://careers.carreker.com/	https://careers.carreker.com/	n/a	Header missing	2019-01-29T09:10:56.934Z
x_content_type_options_missing	https://mail.billmatrix.com/	https://mail.billmatrix.com/	n/a	Header missing	2019-01-29T09:10:56.928Z
x_content_type_options_missing	http://careers.carreker.com/	http://careers.carreker.com/	n/a	Header missing	2019-01-29T09:10:56.855Z
x_content_type_options_missing	https://fiservwebsolutions.com/	https://fiservwebsolutions.com/	n/a	Header missing	2019-01-29T09:10:53.876Z
x_content_type_options_missing	https://support.fiservatlanta.net/	https://support.fiservatlanta.net/	n/a	Header missing	2019-01-29T09:10:53.729Z
x_content_type_options_missing	https://alpha.hepsiian.com/	https://alpha.hepsiian.com/	n/a	Header missing	2019-01-29T09:10:53.348Z
x_content_type_options_missing	https://images.hepsiian.com/	https://images.hepsiian.com/	n/a	Header missing	2019-01-29T09:10:52.534Z
x_content_type_options_missing	https://fiservsupport.com/	http://fiservsupport.com/	http://fiservsupport.com/, 302, https://fiservsupport.com/	Header missing	2019-01-29T09:10:51.744Z
x_content_type_options_missing	https://fiservlendingsolutions.com/	https://fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.983Z
x_content_type_options_missing	http://fiservlendingsolutions.com/	http://fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.913Z
x_content_type_options_missing	https://fiservipvpn.com/	https://fiservipvpn.com/	n/a	Header missing	2019-01-29T09:10:50.584Z
x_content_type_options_missing	http://demo.billmatrix.com/	http://demo.billmatrix.com/	n/a	Header missing	2019-01-29T09:10:50.447Z
x_content_type_options_missing	https://www.fiservlendingsolutions.com/	https://www.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.369Z
x_content_type_options_missing	http://mail.fiservlendingsolutions.com/	http://mail.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.349Z
x_content_type_options_missing	http://www.fiservlendingsolutions.com/	http://www.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.285Z
x_content_type_options_missing	https://fiservcws.com/	https://fiservcws.com/	n/a	Header missing	2019-01-29T09:10:50.069Z
x_content_type_options_missing	https://www.careers.fiserv.com/	https://careers.fiserv.com/	https://careers.fiserv.com/, 301,	Header missing	2019-01-29T09:09:27.681Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

			http://www.careers.fiserv.com, 301, https://www.careers.fiserv.com/		
x_content_type_options_missing	https://alabama.fiservls.com/	https://alabama.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.824Z
x_content_type_options_missing	http://alabama.fiservls.com/	http://alabama.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.763Z
x_content_type_options_missing	https://en.fiservls.com/	https://en.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.760Z
x_content_type_options_missing	https://blog.fiservls.com/	https://blog.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.759Z
x_content_type_options_missing	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.742Z
x_content_type_options_missing	https://shop.fiservls.com/	https://shop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.731Z
x_content_type_options_missing	https://bg.fiservls.com/	https://bg.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.726Z
x_content_type_options_missing	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.715Z
x_content_type_options_missing	http://en.fiservls.com/	http://en.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.691Z
x_content_type_options_missing	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.691Z
x_content_type_options_missing	http://blog.fiservls.com/	http://blog.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.677Z
x_content_type_options_missing	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.662Z
x_content_type_options_missing	http://shop.fiservls.com/	http://shop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.662Z
x_content_type_options_missing	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.646Z
x_content_type_options_missing	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.968Z
x_content_type_options_missing	https://in.fiservls.com/	https://in.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.961Z
x_content_type_options_missing	https://ww.fiservls.com/	https://ww.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.955Z
x_content_type_options_missing	https://chat.fiservls.com/	https://chat.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z
x_content_type_options_missing	https://espanol.fiservls.com/	https://espanol.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z
x_content_type_options_missing	https://backend.fiservls.com/	https://backend.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_content_type_options_missing	https://arizona.fiservls.com/	https://arizona.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.918Z
x_content_type_options_missing	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_content_type_options_missing	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_content_type_options_missing	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_content_type_options_missing	http://download.fiservls.com/	http://download.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_content_type_options_missing	http://in.fiservls.com/	http://in.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.878Z
x_content_type_options_missing	http://backend.fiservls.com/	http://backend.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.878Z
x_content_type_options_missing	http://espanol.fiservls.com/	http://espanol.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.863Z
x_content_type_options_missing	http://forums.fiservls.com/	http://forums.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.853Z
x_content_type_options_missing	http://chat.fiservls.com/	http://chat.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.849Z
x_content_type_options_missing	http://arizona.fiservls.com/	http://arizona.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.849Z
x_content_type_options_missing	https://14.fiservls.com/	https://14.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.091Z
x_content_type_options_missing	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.089Z
x_content_type_options_missing	https://sadmin.fiservls.com/	https://sadmin.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.085Z
x_content_type_options_missing	https://boston.fiservls.com/	https://boston.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.083Z
x_content_type_options_missing	https://developer.fiservls.com/	https://developer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.073Z
x_content_type_options_missing	https://act.fiservls.com/	https://act.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.070Z
x_content_type_options_missing	https://arlington.fiservls.com/	https://arlington.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.063Z
x_content_type_options_missing	https://client.fiservls.com/	https://client.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.063Z
x_content_type_options_missing	https://ftp.fiservls.com/	https://ftp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.047Z
x_content_type_options_missing	http://mobile.fiservls.com/	http://mobile.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.017Z
x_content_type_optio	http://14.fiservls.com/	http://14.fiservls.com/	n/a	Header missing	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

ns_missing					22T07:04:14.016Z
x_content_type_options_missing	http://boston.fiservls.com/	http://boston.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.015Z
x_content_type_options_missing	http://sadmin.fiservls.com/	http://sadmin.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.014Z
x_content_type_options_missing	http://developer.fiservls.com/	http://developer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.993Z
x_content_type_options_missing	http://act.fiservls.com/	http://act.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.993Z
x_content_type_options_missing	http://client.fiservls.com/	http://client.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.990Z
x_content_type_options_missing	http://backup.fiservls.com/	http://backup.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.984Z
x_content_type_options_missing	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.780Z
x_content_type_options_missing	https://blackberry.fiservls.com/	https://blackberry.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.296Z
x_content_type_options_missing	https://citrix.fiservls.com/	https://citrix.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.214Z
x_content_type_options_missing	https://arkansas.fiservls.com/	https://arkansas.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.209Z
x_content_type_options_missing	https://biz.fiservls.com/	https://biz.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.207Z
x_content_type_options_missing	http://citrix.fiservls.com/	http://citrix.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_content_type_options_missing	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_content_type_options_missing	http://arkansas.fiservls.com/	http://arkansas.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_content_type_options_missing	http://blackberry.fiservls.com/	http://blackberry.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_content_type_options_missing	https://demo.fiservls.com/	https://demo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.891Z
x_content_type_options_missing	https://survey.fiservls.com/	https://survey.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.891Z
x_content_type_options_missing	https://au.fiservls.com/	https://au.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.849Z
x_content_type_options_missing	http://survey.fiservls.com/	http://survey.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.815Z
x_content_type_options_missing	http://demo.fiservls.com/	http://demo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.815Z
x_content_type_options_missing	http://arlington.fiservls.com/	http://arlington.fiservls.com/	n/a	Header missing	2019-01-22T07:04:05.405Z

x_content_type_options_missing	http://fiservdox.com/	http://fiservdox.com/	n/a	Header missing	2019-01-22T07:04:03.821Z
x_content_type_options_missing	https://team.fiservls.com/	https://team.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.075Z
x_content_type_options_missing	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.053Z
x_content_type_options_missing	http://mail.fiservls.com/	http://mail.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.030Z
x_content_type_options_missing	http://team.fiservls.com/	http://team.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.013Z
x_content_type_options_missing	https://ns1.fiservls.com/	https://ns1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.005Z
x_content_type_options_missing	https://131.fiservls.com/	https://131.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.976Z
x_content_type_options_missing	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.968Z
x_content_type_options_missing	https://forums.fiservls.com/	https://forums.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.940Z
x_content_type_options_missing	http://pop.fiservls.com/	http://pop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.920Z
x_content_type_options_missing	https://corp.fiservls.com/	https://corp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.904Z
x_content_type_options_missing	http://131.fiservls.com/	http://131.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.897Z
x_content_type_options_missing	https://apps.fiservls.com/	https://apps.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.857Z
x_content_type_options_missing	https://atlanta.fiservls.com/	https://atlanta.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.851Z
x_content_type_options_missing	http://corp.fiservls.com/	http://corp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.819Z
x_content_type_options_missing	http://apps.fiservls.com/	http://apps.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.789Z
x_content_type_options_missing	https://customer.fiservls.com/	https://customer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.784Z
x_content_type_options_missing	https://intranet1.fiservls.com/	https://intranet1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.756Z
x_content_type_options_missing	http://atlanta.fiservls.com/	http://atlanta.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.748Z
x_content_type_options_missing	https://18.fiservls.com/	https://18.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.716Z
x_content_type_options_missing	http://customer.fiservls.com/	http://customer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.710Z
x_content_type_optio	https://administrador.fi	https://administrador.fi	n/a	Header missing	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

ns_missing	servls.com/	servls.com/			22T07:04:02.681Z
x_content_type_options_missing	http://intranet1.fiservls.com/	http://intranet1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.673Z
x_content_type_options_missing	http://18.fiservls.com/	http://18.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.638Z
x_content_type_options_missing	http://administrador.fisfiservls.com/	http://administrador.fisfiservls.com/	n/a	Header missing	2019-01-22T07:04:02.606Z
x_content_type_options_missing	https://backup.fiservls.com/	https://backup.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.590Z
x_content_type_options_missing	https://apollo.fiservls.com/	https://apollo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.577Z
x_content_type_options_missing	https://manage.fiservls.com/	https://manage.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.496Z
x_content_type_options_missing	http://apollo.fiservls.com/	http://apollo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.487Z
x_content_type_options_missing	https://support.fiservls.com/	https://support.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.457Z
x_content_type_options_missing	http://manage.fiservls.com/	http://manage.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.415Z
x_content_type_options_missing	http://au.fiservls.com/	http://au.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.382Z
x_content_type_options_missing	http://support.fiservls.com/	http://support.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.382Z
x_content_type_options_missing	https://email.fiservls.com/	https://email.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.113Z
x_content_type_options_missing	https://ad.fiservls.com/	https://ad.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.039Z
x_content_type_options_missing	http://email.fiservls.com/	http://email.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.030Z
x_content_type_options_missing	https://download.fiservls.com/	https://download.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.000Z
x_content_type_options_missing	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.957Z
x_content_type_options_missing	https://am.fiservls.com/	https://am.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.913Z
x_content_type_options_missing	http://am.fiservls.com/	http://am.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.824Z
x_content_type_options_missing	https://california.fiservls.com/	https://california.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.632Z
x_content_type_options_missing	https://antivirus.fiservls.com/	https://antivirus.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.624Z
x_content_type_options_missing	https://ajax.fiservls.com/	https://ajax.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.621Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_content_type_options_missing	https://pop.fiservls.com/	https://pop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.617Z
x_content_type_options_missing	https://mail.fiservls.com/	https://mail.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.617Z
x_content_type_options_missing	http://antivirus.fiservls.com/	http://antivirus.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z
x_content_type_options_missing	http://ajax.fiservls.com/	http://ajax.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z
x_content_type_options_missing	http://california.fiservls.com/	http://california.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z

RECOMMENDATION

Add the following header to responses from this website: 'X-Content-Type-Options: nosniff'

ABOUT THIS ISSUE

A MIME type is an HTTP header that indicates the type of content returned in a response and how it should be handled and displayed by the browser. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. The X-Content-Type-Options header indicates that browsers should always trust the declared MIME type from the server and not attempt to analyze the content themselves.

APPLICATION SECURITY > ISSUE DETAIL

✓ Web Application Firewall (WAF) Detected

A web application firewall (WAF) monitors traffic to and from a web application, and attempts to detect and block traffic associated with common malicious behaviors. A WAF is an important defensive layer that helps secure your web application.

6 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
barracuda_application_firewall	https://mail.efiserv.com/	https://mail.efiserv.com/	n/a	-	2019-01-29T09:11:04.792Z
Evidence: Barracuda Application Firewall detected with 25% confidence.					
barracuda_application_firewall	https://www.efiserv.com/	https://www.efiserv.com/	n/a	-	2019-01-29T09:11:04.467Z
Evidence: Barracuda Application Firewall detected with 25% confidence.					
f5_big_ip_ltm	https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3a%2f%2flogin.microsoftonline.com%2fte%2ffiservservicepoint.onmicrosoft.com%2fb2c_1	http://my.carreker.com/	http://my.carreker.com/, 302, https://c3.fiserv.com/, 302, https://servicepoint.fiservapps.com/, 302, https://fiserv.service-now.com/, 302,	-	2019-01-29T09:11:00.692Z

	a_prod_sn_signin%2fsamlp%2fsso%2flogin%3fsamlrequest%3dlvlbbptaep0vthdgoxfjvsyssvxvupki2o2hf2sdg7mszjcdhsr%252fx8akts%252bwep15896bn7ni3drxq7lopeedphfaznttamr17qsis6his2gfugfwrld77o5wxyfursvhbdxcy5jboko4iesuabsh25scfj7cpuljuzzvgfzmapubn1s%252b0ktquboi7lt9gqak4w0hawb1ypr3rqatwaaxhswmyhhwbmeadtctzpwtgxqb4qd2qt3em2ouhxnl5zhxyoaebsnxwtzkpjo%252f8l6rlwbkihwvrhmet9umyn%252b%252fwzz6uutfnxyvchlheqrf4ssyizfy%252buqxquqa5fwzmx5s4ww3tjj3sen2gl0qyhklvoz8odnirewrkjk4sulfwsvncg8mlgzpl%252fn%252bpinyft8ccj%252f%252fst9mbl0pwd4p6p%252bk%252bhdynmiemmv6nd1btbbt5xe47ei%252f312sl0uvws8cs1yrrte7bu61kd68rk7pzwnbu48yh5s02l32mfzm6vctvlxjwuwanqjxs%252bq%252fd77%252baw%253d%253d%26relaystate%3dhttps%253a%252f%252ffiserv.service-now.com%252fnavpage.do		https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3A%2F%2Flogin.microsoftonline.com%2Fte%2Ffiservservicepoint.onmicrosoft.com%2FB2C_1A_Prod_sn_signin%2Fsamlp%2Fsso%2Flogin%3FSAMLRequest%3DlVLBbptAEP0VtHdgoXFjVsYSsVXVUpKi2O2hF2sDg7MSzJCdhSR%252FX8AkTS%252BWep15896bN7Ni3dRxq7LOPeEDPHfAznttamR17qSis6hIs2GFugFWrlD77O5WxYFUrSVHBdXCy5jBOkO4IeSuAbsH25sCfj7cpuLJuZZVGFZmAPUBn1s%252B0ktQUBOi7lt9gqAk4W0HAwb1yPR3rqaTwaAxhSWmyhHWBmEadTCTzpwtGXQB4Qd2Qt3Em2OUHXNL5ZHxyOaEBsNxwTZkpjO%252F8L6RLWBKIhWVrhmEt9umYn%252B%252FWZZ6UUTFNXyVchlHEqrF4ssyiZfy%252BuqxquQA5Fwzmx5S4Ww3TjJ3sEN2Gl0qYhklvoz8ODnIREWRkjK4SuLfwsvnCG8MlgZPl%252FN%252BPINYfT8ccj%252F%252FsT9MBL0pwd4P6P%252BK%252BhdYnmIemMV6Nd1bTbbt5xe47Ei%252F312sL0uvws8Cs1yrRte7bU61Kd68rK7pZWNBu48Yh5s02l32MFZM6VcTVLXjWuwAnQjXs%252Bq%252FD77%252BAw%253D%253D%26RelayState%3Dhttps%253A%252F%252Ffiserv.service-now.com%252Fnavpage.do		
Evidence: F5 BIG-IP LTM detected with 25% confidence.					
citrix_netscaler	https://my.carreker.com/login.asp	https://my.carreker.com/	https://my.carreker.com/, 302, https://my.carreker.com/Login.asp	-	2019-01-29T09:10:59.822Z
Evidence: Citrix NetScaler detected with 25% confidence.					
citrix_netscaler	https://fiservdm.net/vpn/index.html	https://fiservdm.net/	https://fiservdm.net/, 302,	-	2019-01-29T09:10:55.671Z

			https://fiservdm.net/vpn/index.html		
Evidence: Citrix NetScaler detected with 25% confidence.					
citrix_netscaler	https://fiservdmdr.net/vpn/index.html	https://fiservdmdr.net/	https://fiservdmdr.net/, 302, https://fiservdmdr.net/vpn/index.html	-	2019-01-29T09:10:49.321Z
Evidence: Citrix NetScaler detected with 25% confidence.					

RECOMMENDATION

Companies should consider implementing a web application firewall that can protect against common web vulnerabilities, such as SQL Injection and cross-site scripting (XSS). Many hosting providers offer WAF capabilities as well.

ABOUT THIS ISSUE

A well configured WAF can detect and block a wide variety of attacks. Capabilities vary between products, but at minimum most WAFs can block SQL injection and Cross Site Scripting attacks. A WAF is no substitute to a well-designed web application that is not vulnerable to these attacks in the first place, but it still plays an important roll in providing layered security.

APPLICATION SECURITY > ISSUE DETAIL

Content Security Policy (CSP) Missing

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

145 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
csp_no_policy	https://staging.fiserv-ecomhosting.com/	https://staging.fiserv-ecomhosting.com/	n/a	-	2019-01-29T09:11:43.731Z
Evidence: No content security policy directives found.					
csp_no_policy	http://services.fiserv-ecomhosting.com/	http://services.fiserv-ecomhosting.com/	n/a	-	2019-01-29T09:11:43.673Z
Evidence: No content security policy directives found.					
csp_no_policy	http://staging.fiserv-ecomhosting.com/	http://staging.fiserv-ecomhosting.com/	n/a	-	2019-01-29T09:11:43.673Z
Evidence: No content security policy directives found.					
csp_no_policy	http://www.fiservsw.com/	http://www.fiservsw.com/	n/a	-	2019-01-29T09:11:42.823Z
Evidence: No content security policy directives found.					

csp_no_policy	https://mail.fiservlendingsolutions.com/	https://mail.fiservlendingsolutions.com/	n/a	-	2019-01-29T09:11:17.099Z
Evidence: No content security policy directives found.					
csp_no_policy	http://fiservcreditservices.com/	http://fiservcreditservices.com/	n/a	-	2019-01-29T09:11:15.569Z
Evidence: No content security policy directives found.					
csp_no_policy	https://webmail.fiserv.net/	https://webmail.fiserv.net/	n/a	-	2019-01-29T09:11:13.849Z
Evidence: No content security policy directives found.					
csp_no_policy	http://fiservsw.com/	http://fiservsw.com/	n/a	-	2019-01-29T09:11:05.384Z
Evidence: No content security policy directives found.					
csp_no_policy	https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3a%2f%2flogin.microsoftonline.com%2fte%2ffiservservicepoint.onmicrosoft.com%2fb2c_1a_prod_sn_signin%2fsamlp%2fsso%2flogin%3fsamlrequest%3dlvlbbptaep0vthdgoxfjvsyssvxvupki2o2hf2sdg7mszjcdhsr%252fx8akts%252bwep15896bn7ni3drxq7lopeedphfaznttamr17qsis6his2gfugfwrld77o5wxyfursvhbdxcy5jboko4iesuabsh25scfj7cpuljuzzvgfzmapubn1s%252b0ktquboi7lt9gqak4w0hawb1ypr3rqatwaaxhswmyhhwbmeadtctzpwtgxqb4qd2qt3em2ouhxnl5zhxyoaebsnxwtzkpjo%252f8l6rlwbkihwvrhmet9umyn%252b%252fwzz6uutfnxyvchlheqrf4ssyizfy%252buqxquqa5fwzmx5s4ww3tjj3sen2gl0qyhklvoz8odnirewrkjk4sulfwsvncg8mlgzpl%252fn%252bpinyft8ccj%252f%252fst9mbl0pwd4p6p%252bk%252bhdynmiemmv6nd1btbbt5xe47ei%252f312sl0uvws8cs1yrrte7bu61kd68rk7pzwnbu48yh5s02l32mfzm6vctvlxjwuwanqjxs%252bq%252fd77%252baw%253d%253d	http://my.carreker.com/	http://my.carreker.com/, 302, https://c3.fiserv.com/, 302, https://servicepoint.fiservapps.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3A%2F%2Flogin.microsoftonline.com%2Fte%2Ffiservservicepoint.onmicrosoft.com%2FB2C_1A_Prod_sn_signin%2Fsamlp%2Fsso%2Flogin%3FSAMLRequest%3DlVLBbptAEP0VtHdgoXFjVsYSsVXVUpKi2O2hF2sDg7MSzJCdhSR%252FX8AkTS%252BWep15896bN7Ni3dRxq7LOPeEDPHfAznttamR17qSis6hls2GFugFWrlD77O5WxYFUrSVHBdXCy5jBOkO4leSuAbsH25sCfj7cpuLJuZZVGFZmAPUBn1s%252B0ktQUBOi7lt9gqAk4W0HAwb1yPR3rqaTwaAxhSWmyhHWBmEadTCTzpwtGXQB4Qd2Qt3Em2OUHXNL5ZHxyOaEBsNxwTZkpjO%252F8L6RLWBKlhWVrhmEt9umYn%252B%252FWZZ6UUTFNXyVchlHEqrF4ssyiZfy%252BuqxquQA5Fwzmx5S4Ww3TjJ3sEN2Gl0qYhklvoz8ODnIREWRkjK4SuLfwsvnCG8Ml	-	2019-01-29T09:11:00.692Z

	%26relaystate%3dhttps%253a%252f%252ffiserv.service-now.com%252fnavpage.do		gZPI%252FN%252BPINYfT8ccj%252F%252FsT9MBL0pwd4P6P%252BK%252BhdYnmIemMV6Nd1bTbbt5xe47Ei%252F312sL0uvws8Cs1yrRte7bU61Kd68rK7pZWNBu48Yh5s02I32MFZM6VcTVLXjWuwAnQjXs%252Bq%252FD77%252BAw%253D%253D%26RelayState%3Dhttps%253A%252F%252Ffiserv.service-now.com%252Fnavpage.do		
Evidence: No content security policy directives found.					
csp_no_policy	https://search.carreker.com/	https://search.carreker.com/	n/a	-	2019-01-29T09:10:57.094Z
Evidence: No content security policy directives found.					
csp_no_policy	http://search.carreker.com/	http://search.carreker.com/	n/a	-	2019-01-29T09:10:57.065Z
Evidence: No content security policy directives found.					
csp_no_policy	https://careers.carreker.com/	https://careers.carreker.com/	n/a	-	2019-01-29T09:10:56.934Z
Evidence: No content security policy directives found.					
csp_no_policy	https://mail.billmatrix.com/	https://mail.billmatrix.com/	n/a	-	2019-01-29T09:10:56.928Z
Evidence: No content security policy directives found.					
csp_no_policy	http://careers.carreker.com/	http://careers.carreker.com/	n/a	-	2019-01-29T09:10:56.855Z
Evidence: No content security policy directives found.					
csp_no_policy	https://fiserv-ecomhosting.com/logon.asp	https://fiserv-ecomhosting.com/	https://fiserv-ecomhosting.com/, 302, https://fiserv-ecomhosting.com/logon.asp	-	2019-01-29T09:10:53.901Z
Evidence: block-all-mixed-content					
csp_no_policy	https://fiservwebsolutions.com/	https://fiservwebsolutions.com/	n/a	-	2019-01-29T09:10:53.876Z
Evidence: No content security policy directives found.					
csp_no_policy	https://support.fiservatlanta.net/	https://support.fiservatlanta.net/	n/a	-	2019-01-29T09:10:53.729Z

Evidence: No content security policy directives found.					
csp_no_policy	https://www.fiserv-ecomhosting.com/logon.asp	https://www.fiserv-ecomhosting.com/	https://www.fiserv-ecomhosting.com/, 302, https://www.fiserv-ecomhosting.com/logon.asp	-	2019-01-29T09:10:53.673Z
Evidence: block-all-mixed-content					
csp_no_policy	https://alpha.hepsiian.com/	https://alpha.hepsiian.com/	n/a	-	2019-01-29T09:10:53.348Z
Evidence: No content security policy directives found.					
csp_no_policy	https://auth01.client-central.com/nidp/idff/sso?requestid=iduqs0f5e4nosmhposwxxb8jculjy&majorversion=1&minorversion=2&issueinstant=2019-01-29t09%3a10%3a52z&providerid=https%3a%2f%2fwww.client-central.com%3a443%2fnesp%2fidff%2fmetadata&relaystate=ma%3d%3d&consent=urn%3aliberty%3aconsent%3aunavailable&agappna=clientcentral_home&forceauthn=false&ispassive=false&nameidpolicy=onetime&protocolprofile=http%3a%2f%2fprojectliberty.org%2fprofiles%2fbrws-art&target=https%3a%2f%2fwww.fiserveft.com%2f&authncontextstatementref=radius%2ftoken%2furi	https://www.fiserveft.com/	https://www.fiserveft.com/, 302, https://www.client-central.com:443/nesp/app/plogin?agAppNa=clientCentral_Home&c=radius/token/uri&target=%22https://www.fiserveft.com/%22, 302, https://auth01.client-central.com/nidp/idff/sso?RequestID=idUQS0F5E4NOSmHPOsWxXB8jCUljY&MajorVersion=1&MinorVersion=2&IssueInstant=2019-01-29T09%3A10%3A52Z&ProviderID=https%3A%2F%2Fwww.client-central.com%3A443%2Fnesp%2Fidff%2Fmetadata&RelayState=MA%3D%3D&consent=urn%3Aliberty%3Aconsent%3Aunavailable&agAppNa=clientCentral_Home&ForceAuthn=false&IsPassive=false&NameIDPolicy=onetime&ProtocolProfile=http%3A%2F%2Fprojectliberty.org%2Fprofiles%2Fbrws-art&target=https%3A%2F%2Fwww.fiserveft.com%2F&AuthnContextStatementRef=radius%2Ftoken%2Furi	-	2019-01-29T09:10:53.019Z
Evidence: No content security policy directives found.					
csp_no_policy	https://images.hepsiian.com/	https://images.hepsiian.com/	n/a	-	2019-01-29T09:10:52.534Z
Evidence:					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

No content security policy directives found.					
csp_no_policy	https://news.checkfree.com/	https://news.checkfree.com/	n/a	-	2019-01-29T09:10:52.427Z
Evidence: No content security policy directives found.					
csp_no_policy	https://www.fiservwebsolutions.com	http://fiservwebsolutions.com/	http://fiservwebsolutions.com/, 301, https://www.fiservwebsolutions.com	-	2019-01-29T09:10:52.406Z
Evidence: block-all-mixed-content					
csp_no_policy	https://fiservsupport.com/	http://fiservsupport.com/	http://fiservsupport.com/, 302, https://fiservsupport.com/	-	2019-01-29T09:10:51.744Z
Evidence: No content security policy directives found.					
csp_no_policy	https://fiservlendingsolutions.com/	https://fiservlendingsolutions.com/	n/a	-	2019-01-29T09:10:50.983Z
Evidence: No content security policy directives found.					
csp_no_policy	http://fiservlendingsolutions.com/	http://fiservlendingsolutions.com/	n/a	-	2019-01-29T09:10:50.913Z
Evidence: No content security policy directives found.					
csp_no_policy	https://fiservipvpn.com/	https://fiservipvpn.com/	n/a	-	2019-01-29T09:10:50.584Z
Evidence: No content security policy directives found.					
csp_no_policy	http://demo.billmatrix.com/	http://demo.billmatrix.com/	n/a	-	2019-01-29T09:10:50.447Z
Evidence: No content security policy directives found.					
csp_no_policy	https://www.fiservlendingsolutions.com/	https://www.fiservlendingsolutions.com/	n/a	-	2019-01-29T09:10:50.369Z
Evidence: No content security policy directives found.					
csp_no_policy	http://mail.fiservlendingsolutions.com/	http://mail.fiservlendingsolutions.com/	n/a	-	2019-01-29T09:10:50.349Z
Evidence: No content security policy directives found.					
csp_no_policy	http://www.fiservlendingsolutions.com/	http://www.fiservlendingsolutions.com/	n/a	-	2019-01-29T09:10:50.285Z
Evidence: No content security policy directives found.					
csp_no_policy	https://fiservcws.com/	https://fiservcws.com/	n/a	-	2019-01-29T09:10:50.069Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Evidence: No content security policy directives found.					
csp_no_policy	https://www.careers.fiserv.com/	https://careers.fiserv.com/	https://careers.fiserv.com/, 301, http://www.careers.fiserv.com, 301, https://www.careers.fiserv.com/	-	2019-01-29T09:09:27.681Z
Evidence: No content security policy directives found.					
csp_no_policy	https://alabama.fiservls.com/	https://alabama.fiservls.com/	n/a	-	2019-01-22T07:04:16.824Z
Evidence: No content security policy directives found.					
csp_no_policy	http://alabama.fiservls.com/	http://alabama.fiservls.com/	n/a	-	2019-01-22T07:04:16.763Z
Evidence: No content security policy directives found.					
csp_no_policy	https://en.fiservls.com/	https://en.fiservls.com/	n/a	-	2019-01-22T07:04:16.760Z
Evidence: No content security policy directives found.					
csp_no_policy	https://blog.fiservls.com/	https://blog.fiservls.com/	n/a	-	2019-01-22T07:04:16.759Z
Evidence: No content security policy directives found.					
csp_no_policy	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	-	2019-01-22T07:04:16.742Z
Evidence: No content security policy directives found.					
csp_no_policy	https://shop.fiservls.com/	https://shop.fiservls.com/	n/a	-	2019-01-22T07:04:16.731Z
Evidence: No content security policy directives found.					
csp_no_policy	https://bg.fiservls.com/	https://bg.fiservls.com/	n/a	-	2019-01-22T07:04:16.726Z
Evidence: No content security policy directives found.					
csp_no_policy	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	-	2019-01-22T07:04:16.715Z
Evidence: No content security policy directives found.					
csp_no_policy	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	-	2019-01-22T07:04:16.691Z
Evidence: No content security policy directives found.					
csp_no_policy	http://en.fiservls.com/	http://en.fiservls.com/	n/a	-	2019-01-22T07:04:16.691Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Evidence: No content security policy directives found.					
csp_no_policy	http://blog.fiservls.com/	http://blog.fiservls.com/	n/a	-	2019-01-22T07:04:16.677Z
Evidence: No content security policy directives found.					
csp_no_policy	http://shop.fiservls.com/	http://shop.fiservls.com/	n/a	-	2019-01-22T07:04:16.662Z
Evidence: No content security policy directives found.					
csp_no_policy	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	-	2019-01-22T07:04:16.662Z
Evidence: No content security policy directives found.					
csp_no_policy	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	-	2019-01-22T07:04:16.646Z
Evidence: No content security policy directives found.					
csp_no_policy	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	-	2019-01-22T07:04:14.968Z
Evidence: No content security policy directives found.					
csp_no_policy	https://in.fiservls.com/	https://in.fiservls.com/	n/a	-	2019-01-22T07:04:14.961Z
Evidence: No content security policy directives found.					
csp_no_policy	https://ww.fiservls.com/	https://ww.fiservls.com/	n/a	-	2019-01-22T07:04:14.955Z
Evidence: No content security policy directives found.					
csp_no_policy	https://espanol.fiservls.com/	https://espanol.fiservls.com/	n/a	-	2019-01-22T07:04:14.953Z
Evidence: No content security policy directives found.					
csp_no_policy	https://backend.fiservls.com/	https://backend.fiservls.com/	n/a	-	2019-01-22T07:04:14.953Z
Evidence: No content security policy directives found.					
csp_no_policy	https://chat.fiservls.com/	https://chat.fiservls.com/	n/a	-	2019-01-22T07:04:14.953Z
Evidence: No content security policy directives found.					
csp_no_policy	https://arizona.fiservls.com/	https://arizona.fiservls.com/	n/a	-	2019-01-22T07:04:14.918Z
Evidence: No content security policy directives found.					

csp_no_policy	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	-	2019-01-22T07:04:14.897Z
Evidence: No content security policy directives found.					
csp_no_policy	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	-	2019-01-22T07:04:14.897Z
Evidence: No content security policy directives found.					
csp_no_policy	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	-	2019-01-22T07:04:14.897Z
Evidence: No content security policy directives found.					
csp_no_policy	http://download.fiservls.com/	http://download.fiservls.com/	n/a	-	2019-01-22T07:04:14.897Z
Evidence: No content security policy directives found.					
csp_no_policy	http://in.fiservls.com/	http://in.fiservls.com/	n/a	-	2019-01-22T07:04:14.878Z
Evidence: No content security policy directives found.					
csp_no_policy	http://backend.fiservls.com/	http://backend.fiservls.com/	n/a	-	2019-01-22T07:04:14.878Z
Evidence: No content security policy directives found.					
csp_no_policy	http://espanol.fiservls.com/	http://espanol.fiservls.com/	n/a	-	2019-01-22T07:04:14.863Z
Evidence: No content security policy directives found.					
csp_no_policy	http://forums.fiservls.com/	http://forums.fiservls.com/	n/a	-	2019-01-22T07:04:14.853Z
Evidence: No content security policy directives found.					
csp_no_policy	http://chat.fiservls.com/	http://chat.fiservls.com/	n/a	-	2019-01-22T07:04:14.849Z
Evidence: No content security policy directives found.					
csp_no_policy	http://arizona.fiservls.com/	http://arizona.fiservls.com/	n/a	-	2019-01-22T07:04:14.849Z
Evidence: No content security policy directives found.					
csp_no_policy	https://14.fiservls.com/	https://14.fiservls.com/	n/a	-	2019-01-22T07:04:14.091Z
Evidence: No content security policy directives found.					
csp_no_policy	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	-	2019-01-22T07:04:14.089Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Evidence: No content security policy directives found.					
csp_no_policy	https://sadmin.fiservls.com/	https://sadmin.fiservls.com/	n/a	-	2019-01-22T07:04:14.085Z
Evidence: No content security policy directives found.					
csp_no_policy	https://boston.fiservls.com/	https://boston.fiservls.com/	n/a	-	2019-01-22T07:04:14.083Z
Evidence: No content security policy directives found.					
csp_no_policy	https://developer.fiservls.com/	https://developer.fiservls.com/	n/a	-	2019-01-22T07:04:14.073Z
Evidence: No content security policy directives found.					
csp_no_policy	https://act.fiservls.com/	https://act.fiservls.com/	n/a	-	2019-01-22T07:04:14.070Z
Evidence: No content security policy directives found.					
csp_no_policy	https://arlington.fiservls.com/	https://arlington.fiservls.com/	n/a	-	2019-01-22T07:04:14.063Z
Evidence: No content security policy directives found.					
csp_no_policy	https://client.fiservls.com/	https://client.fiservls.com/	n/a	-	2019-01-22T07:04:14.063Z
Evidence: No content security policy directives found.					
csp_no_policy	https://ftp.fiservls.com/	https://ftp.fiservls.com/	n/a	-	2019-01-22T07:04:14.047Z
Evidence: No content security policy directives found.					
csp_no_policy	http://mobile.fiservls.com/	http://mobile.fiservls.com/	n/a	-	2019-01-22T07:04:14.017Z
Evidence: No content security policy directives found.					
csp_no_policy	http://14.fiservls.com/	http://14.fiservls.com/	n/a	-	2019-01-22T07:04:14.016Z
Evidence: No content security policy directives found.					
csp_no_policy	http://boston.fiservls.com/	http://boston.fiservls.com/	n/a	-	2019-01-22T07:04:14.015Z
Evidence: No content security policy directives found.					
csp_no_policy	http://sadmin.fiservls.com/	http://sadmin.fiservls.com/	n/a	-	2019-01-22T07:04:14.014Z
Evidence: No content security policy directives found.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

csp_no_policy	http://developer.fiservls.com/	http://developer.fiservls.com/	n/a	-	2019-01-22T07:04:13.993Z
Evidence: No content security policy directives found.					
csp_no_policy	http://act.fiservls.com/	http://act.fiservls.com/	n/a	-	2019-01-22T07:04:13.993Z
Evidence: No content security policy directives found.					
csp_no_policy	http://client.fiservls.com/	http://client.fiservls.com/	n/a	-	2019-01-22T07:04:13.990Z
Evidence: No content security policy directives found.					
csp_no_policy	http://backup.fiservls.com/	http://backup.fiservls.com/	n/a	-	2019-01-22T07:04:13.984Z
Evidence: No content security policy directives found.					
csp_no_policy	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	-	2019-01-22T07:04:13.780Z
Evidence: No content security policy directives found.					
csp_no_policy	https://blackberry.fiservls.com/	https://blackberry.fiservls.com/	n/a	-	2019-01-22T07:04:13.296Z
Evidence: No content security policy directives found.					
csp_no_policy	https://citrix.fiservls.com/	https://citrix.fiservls.com/	n/a	-	2019-01-22T07:04:13.214Z
Evidence: No content security policy directives found.					
csp_no_policy	https://arkansas.fiservls.com/	https://arkansas.fiservls.com/	n/a	-	2019-01-22T07:04:13.209Z
Evidence: No content security policy directives found.					
csp_no_policy	https://biz.fiservls.com/	https://biz.fiservls.com/	n/a	-	2019-01-22T07:04:13.207Z
Evidence: No content security policy directives found.					
csp_no_policy	http://citrix.fiservls.com/	http://citrix.fiservls.com/	n/a	-	2019-01-22T07:04:13.145Z
Evidence: No content security policy directives found.					
csp_no_policy	http://arkansas.fiservls.com/	http://arkansas.fiservls.com/	n/a	-	2019-01-22T07:04:13.145Z
Evidence: No content security policy directives found.					
csp_no_policy	http://blackberry.fiservls.com/	http://blackberry.fiservls.com/	n/a	-	2019-01-22T07:04:13.145Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Evidence: No content security policy directives found.					
csp_no_policy	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	-	2019-01-22T07:04:13.145Z
Evidence: No content security policy directives found.					
csp_no_policy	https://survey.fiservls.com/	https://survey.fiservls.com/	n/a	-	2019-01-22T07:04:12.891Z
Evidence: No content security policy directives found.					
csp_no_policy	https://demo.fiservls.com/	https://demo.fiservls.com/	n/a	-	2019-01-22T07:04:12.891Z
Evidence: No content security policy directives found.					
csp_no_policy	https://au.fiservls.com/	https://au.fiservls.com/	n/a	-	2019-01-22T07:04:12.849Z
Evidence: No content security policy directives found.					
csp_no_policy	http://demo.fiservls.com/	http://demo.fiservls.com/	n/a	-	2019-01-22T07:04:12.815Z
Evidence: No content security policy directives found.					
csp_no_policy	http://survey.fiservls.com/	http://survey.fiservls.com/	n/a	-	2019-01-22T07:04:12.815Z
Evidence: No content security policy directives found.					
csp_no_policy	https://flagstar-devicemanager-uat.fiservapps.com/	https://flagstar-devicemanager-uat.fiservapps.com/	n/a	-	2019-01-22T07:04:09.273Z
Evidence: No content security policy directives found.					
csp_no_policy	http://arlington.fiservls.com/	http://arlington.fiservls.com/	n/a	-	2019-01-22T07:04:05.405Z
Evidence: No content security policy directives found.					
csp_no_policy	http://fiservdox.com/	http://fiservdox.com/	n/a	-	2019-01-22T07:04:03.821Z
Evidence: No content security policy directives found.					
csp_no_policy	https://team.fiservls.com/	https://team.fiservls.com/	n/a	-	2019-01-22T07:04:03.075Z
Evidence: No content security policy directives found.					
csp_no_policy	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	-	2019-01-22T07:04:03.053Z
Evidence: No content security policy directives found.					

csp_no_policy	http://mail.fiservls.com/	http://mail.fiservls.com/	n/a	-	2019-01-22T07:04:03.030Z
Evidence: No content security policy directives found.					
csp_no_policy	http://team.fiservls.com/	http://team.fiservls.com/	n/a	-	2019-01-22T07:04:03.013Z
Evidence: No content security policy directives found.					
csp_no_policy	https://ns1.fiservls.com/	https://ns1.fiservls.com/	n/a	-	2019-01-22T07:04:03.005Z
Evidence: No content security policy directives found.					
csp_no_policy	https://131.fiservls.com/	https://131.fiservls.com/	n/a	-	2019-01-22T07:04:02.976Z
Evidence: No content security policy directives found.					
csp_no_policy	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	-	2019-01-22T07:04:02.968Z
Evidence: No content security policy directives found.					
csp_no_policy	https://forums.fiservls.com/	https://forums.fiservls.com/	n/a	-	2019-01-22T07:04:02.940Z
Evidence: No content security policy directives found.					
csp_no_policy	http://pop.fiservls.com/	http://pop.fiservls.com/	n/a	-	2019-01-22T07:04:02.920Z
Evidence: No content security policy directives found.					
csp_no_policy	https://corp.fiservls.com/	https://corp.fiservls.com/	n/a	-	2019-01-22T07:04:02.904Z
Evidence: No content security policy directives found.					
csp_no_policy	http://131.fiservls.com/	http://131.fiservls.com/	n/a	-	2019-01-22T07:04:02.897Z
Evidence: No content security policy directives found.					
csp_no_policy	https://apps.fiservls.com/	https://apps.fiservls.com/	n/a	-	2019-01-22T07:04:02.857Z
Evidence: No content security policy directives found.					
csp_no_policy	https://atlanta.fiservls.com/	https://atlanta.fiservls.com/	n/a	-	2019-01-22T07:04:02.851Z
Evidence: No content security policy directives found.					
csp_no_policy	http://corp.fiservls.com/	http://corp.fiservls.com/	n/a	-	2019-01-22T07:04:02.819Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Evidence: No content security policy directives found.					
csp_no_policy	http://apps.fiservls.com/	http://apps.fiservls.com/	n/a	-	2019-01-22T07:04:02.789Z
Evidence: No content security policy directives found.					
csp_no_policy	https://customer.fiservls.com/	https://customer.fiservls.com/	n/a	-	2019-01-22T07:04:02.784Z
Evidence: No content security policy directives found.					
csp_no_policy	https://intranet1.fiservls.com/	https://intranet1.fiservls.com/	n/a	-	2019-01-22T07:04:02.756Z
Evidence: No content security policy directives found.					
csp_no_policy	http://atlanta.fiservls.com/	http://atlanta.fiservls.com/	n/a	-	2019-01-22T07:04:02.748Z
Evidence: No content security policy directives found.					
csp_no_policy	https://18.fiservls.com/	https://18.fiservls.com/	n/a	-	2019-01-22T07:04:02.716Z
Evidence: No content security policy directives found.					
csp_no_policy	http://customer.fiservls.com/	http://customer.fiservls.com/	n/a	-	2019-01-22T07:04:02.710Z
Evidence: No content security policy directives found.					
csp_no_policy	https://administrador.fiservls.com/	https://administrador.fiservls.com/	n/a	-	2019-01-22T07:04:02.681Z
Evidence: No content security policy directives found.					
csp_no_policy	http://intranet1.fiservls.com/	http://intranet1.fiservls.com/	n/a	-	2019-01-22T07:04:02.673Z
Evidence: No content security policy directives found.					
csp_no_policy	http://18.fiservls.com/	http://18.fiservls.com/	n/a	-	2019-01-22T07:04:02.638Z
Evidence: No content security policy directives found.					
csp_no_policy	http://administrador.fiservls.com/	http://administrador.fiservls.com/	n/a	-	2019-01-22T07:04:02.606Z
Evidence: No content security policy directives found.					
csp_no_policy	https://backup.fiservls.com/	https://backup.fiservls.com/	n/a	-	2019-01-22T07:04:02.590Z
Evidence: No content security policy directives found.					

csp_no_policy	https://apollo.fiservls.com/	https://apollo.fiservls.com/	n/a	-	2019-01-22T07:04:02.577Z
Evidence: No content security policy directives found.					
csp_no_policy	https://manage.fiservls.com/	https://manage.fiservls.com/	n/a	-	2019-01-22T07:04:02.496Z
Evidence: No content security policy directives found.					
csp_no_policy	http://apollo.fiservls.com/	http://apollo.fiservls.com/	n/a	-	2019-01-22T07:04:02.487Z
Evidence: No content security policy directives found.					
csp_no_policy	https://support.fiservls.com/	https://support.fiservls.com/	n/a	-	2019-01-22T07:04:02.457Z
Evidence: No content security policy directives found.					
csp_no_policy	http://manage.fiservls.com/	http://manage.fiservls.com/	n/a	-	2019-01-22T07:04:02.415Z
Evidence: No content security policy directives found.					
csp_no_policy	http://au.fiservls.com/	http://au.fiservls.com/	n/a	-	2019-01-22T07:04:02.382Z
Evidence: No content security policy directives found.					
csp_no_policy	http://support.fiservls.com/	http://support.fiservls.com/	n/a	-	2019-01-22T07:04:02.382Z
Evidence: No content security policy directives found.					
csp_no_policy	https://email.fiservls.com/	https://email.fiservls.com/	n/a	-	2019-01-22T07:04:02.113Z
Evidence: No content security policy directives found.					
csp_no_policy	https://ad.fiservls.com/	https://ad.fiservls.com/	n/a	-	2019-01-22T07:04:02.039Z
Evidence: No content security policy directives found.					
csp_no_policy	http://email.fiservls.com/	http://email.fiservls.com/	n/a	-	2019-01-22T07:04:02.030Z
Evidence: No content security policy directives found.					
csp_no_policy	https://download.fiservls.com/	https://download.fiservls.com/	n/a	-	2019-01-22T07:04:02.000Z
Evidence: No content security policy directives found.					
csp_no_policy	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	-	2019-01-22T07:04:01.957Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Evidence: No content security policy directives found.					
csp_no_policy	https://am.fiservls.com/	https://am.fiservls.com/	n/a	-	2019-01-22T07:04:01.913Z
Evidence: No content security policy directives found.					
csp_no_policy	http://am.fiservls.com/	http://am.fiservls.com/	n/a	-	2019-01-22T07:04:01.824Z
Evidence: No content security policy directives found.					
csp_no_policy	https://california.fiservls.com/	https://california.fiservls.com/	n/a	-	2019-01-22T07:04:01.632Z
Evidence: No content security policy directives found.					
csp_no_policy	https://antivirus.fiservls.com/	https://antivirus.fiservls.com/	n/a	-	2019-01-22T07:04:01.624Z
Evidence: No content security policy directives found.					
csp_no_policy	https://ajax.fiservls.com/	https://ajax.fiservls.com/	n/a	-	2019-01-22T07:04:01.621Z
Evidence: No content security policy directives found.					
csp_no_policy	https://mail.fiservls.com/	https://mail.fiservls.com/	n/a	-	2019-01-22T07:04:01.617Z
Evidence: No content security policy directives found.					
csp_no_policy	https://pop.fiservls.com/	https://pop.fiservls.com/	n/a	-	2019-01-22T07:04:01.617Z
Evidence: No content security policy directives found.					
csp_no_policy	http://ajax.fiservls.com/	http://ajax.fiservls.com/	n/a	-	2019-01-22T07:04:01.560Z
Evidence: No content security policy directives found.					
csp_no_policy	http://california.fiservls.com/	http://california.fiservls.com/	n/a	-	2019-01-22T07:04:01.560Z
Evidence: No content security policy directives found.					
csp_no_policy	http://antivirus.fiservls.com/	http://antivirus.fiservls.com/	n/a	-	2019-01-22T07:04:01.560Z
Evidence: No content security policy directives found.					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

RECOMMENDATION

Enable CSP headers via your webserver configuration.

ABOUT THIS ISSUE

The Content Security Policy provides a valuable safety net that protects your website from malicious cross-site scripting (XSS) attacks. A well configured policy will stop an attacker attempting to inject their code, or references to other malicious content, into your website. Without a Content Security Policy, it's easy for website developers to make mistakes that allow an attacker to inject content that changes the way the website behaves.

APPLICATION SECURITY > ISSUE DETAIL

ⓘ Content Security Policy Contains Broad Directives

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

1 finding

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
csp_too_broad	https://my.carreker.com/login.asp	https://my.carreker.com/	https://my.carreker.com/, 302, https://my.carreker.com/Login.asp	-	2019-01-29T09:10:59.822Z

Evidence:
"frame-ancestors c3.fiserv.com facets.fiserv.com","default-src 'self' ; img-src 'self' 'data' ; connect-src 'self' 'wss' ; report-uri https://report-uri.io/report/URL;"

RECOMMENDATION

Explicitly specify trusted sources for your script-src and object-src policies. Ideally you can use the 'self' directive to limit scripts and objects to only those on your own domain, or you can explicitly specify domains that you trust and rely upon for your site to function.

ABOUT THIS ISSUE

The Content Security Policy (CSP) header can mitigate Cross-Site Scripting (XSS) attacks by prohibiting the browser from loading resources on your page from domains that you don't explicitly trust. However, by using overly broad methods of describing what you trust (ie. 'http:', '*', 'http://*') for your script-src and object-src directives, or your default-src directive in the absence of those directives, this key feature of the CSP header can be bypassed by an attacker.

APPLICATION SECURITY > ISSUE DETAIL

ⓘ Content Security Policy Contains 'unsafe-*' Directive

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

9 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

<table>
<tr><td>csp_unsafe_policy</td><td>http://agility-fiserv.com/</td><td>http://agility-fiserv.com/</td><td>n/a</td><td>-</td><td>2019-01-29T09:10:55.566Z</td></tr>
<tr><td colspan="6">Evidence:
default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://ion.fiserv.com https://connect.facebook.net www.youtube.com https://players.brightcove.net https://hls.cf.brightcove.com https://fonts.gstatic.com https://fonts.googleapis.com https://cdn.hypemarks.com www.digitalfileshares.com https://brightcove.hs.llnwd.net www.fiserv.com https://www.fiserv.com https://vjs.zencdn.net https://www.google.ca https://*.addthis.com https://www.google.com https://secure.brightcove.com https://f1.media.brightcove.com data: https://metrics.brightcove.com https://edge.api.brightcove.com blob: https://*.doubleclick.net https://www.google.com https://8174811.fls.doubleclick.net https://www.google-analytics.com https://t.co https://stats.g.doubleclick.net https://vlog.leadformix.com https://www.facebook.com https://secure.adnxs.com https://www.pages05.net https://*.pingdom.net https://*.linkedin.com 'unsafe-inline' 'unsafe-eval'; script-src https://tagmanager.google.com https://ajax.googleapis.com https://8f2a3f802cdf2859af9e-51128641de34f0801c2bd5e1e5f0dc25.ssl.cf1.rackcdn.com https://api.keen.io https://www.fiserv.com https://s.ytimg.com https://www.youtube.com https://www.tintup.com https://*.cloudfront.net www.fiserv.com https://www.googletagmanager.com https://*.addthis.com https://m.addthisedge.com https://www.sc.pages05.net https://www.google-analytics.com https://sjs.bizographics.com https://static.ads-twitter.com https://*.pingdom.net https://snap.licdn.com https://vlog.leadformix.com https://*.facebook.com https://*.twitter.com https://www.google.com https://*.facebook.net https://*.linkedin.com https://*.adnxs.com https://players.brightcove.net https://vjs.zencdn.net https://www.fiserv.com blob: https://www.bizographics.com 'unsafe-inline' 'unsafe-eval'</td></tr>
<tr><td>csp_unsafe_policy</td><td>https://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx</td><td>http://fiserv-galaxy.com/</td><td>http://fiserv-galaxy.com/, 302, http://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx, 302, https://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx</td><td>-</td><td>2019-01-29T09:10:54.588Z</td></tr>
<tr><td colspan="6">Evidence:
default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://ion.fiserv.com https://connect.facebook.net www.youtube.com https://players.brightcove.net https://hls.cf.brightcove.com https://fonts.gstatic.com https://fonts.googleapis.com https://cdn.hypemarks.com www.digitalfileshares.com https://brightcove.hs.llnwd.net www.fiserv.com https://www.fiserv.com https://vjs.zencdn.net https://www.google.ca https://*.addthis.com https://www.google.com https://secure.brightcove.com https://f1.media.brightcove.com data: https://metrics.brightcove.com https://edge.api.brightcove.com blob: https://*.doubleclick.net https://www.google.com https://8174811.fls.doubleclick.net https://www.google-analytics.com https://t.co https://stats.g.doubleclick.net https://vlog.leadformix.com https://www.facebook.com https://secure.adnxs.com https://www.pages05.net https://*.pingdom.net https://*.linkedin.com 'unsafe-inline' 'unsafe-eval'; script-src https://tagmanager.google.com https://ajax.googleapis.com https://8f2a3f802cdf2859af9e-51128641de34f0801c2bd5e1e5f0dc25.ssl.cf1.rackcdn.com https://api.keen.io https://www.fiserv.com https://s.ytimg.com https://www.youtube.com https://www.tintup.com https://*.cloudfront.net www.fiserv.com https://www.googletagmanager.com https://*.addthis.com https://m.addthisedge.com https://www.sc.pages05.net https://www.google-analytics.com https://sjs.bizographics.com https://static.ads-twitter.com https://*.pingdom.net https://snap.licdn.com https://vlog.leadformix.com https://*.facebook.com https://*.twitter.com https://www.google.com https://*.facebook.net https://*.linkedin.com https://*.adnxs.com https://players.brightcove.net https://vjs.zencdn.net https://www.fiserv.com blob: https://www.bizographics.com 'unsafe-inline' 'unsafe-eval'</td></tr>
<tr><td>csp_unsafe_policy</td><td>http://bbs.summitsite.com/</td><td>http://bbs.summitsite.com/</td><td>n/a</td><td>-</td><td>2019-01-29T09:10:53.790Z</td></tr>
<tr><td colspan="6">Evidence:
default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://ion.fiserv.com https://connect.facebook.net www.youtube.com https://players.brightcove.net https://hls.cf.brightcove.com https://fonts.gstatic.com https://fonts.googleapis.com https://cdn.hypemarks.com www.digitalfileshares.com https://brightcove.hs.llnwd.net www.fiserv.com https://www.fiserv.com https://vjs.zencdn.net https://www.google.ca https://*.addthis.com https://www.google.com https://secure.brightcove.com https://f1.media.brightcove.com data: https://metrics.brightcove.com https://edge.api.brightcove.com blob: https://*.doubleclick.net https://www.google.com https://8174811.fls.doubleclick.net https://www.google-analytics.com https://t.co https://stats.g.doubleclick.net https://vlog.leadformix.com https://www.facebook.com https://secure.adnxs.com https://www.pages05.net https://*.pingdom.net https://*.linkedin.com 'unsafe-inline' 'unsafe-eval'; script-src https://tagmanager.google.com https://ajax.googleapis.com https://8f2a3f802cdf2859af9e-51128641de34f0801c2bd5e1e5f0dc25.ssl.cf1.rackcdn.com https://api.keen.io https://www.fiserv.com https://s.ytimg.com https://www.youtube.com https://www.tintup.com https://*.cloudfront.net www.fiserv.com https://www.googletagmanager.com https://*.addthis.com https://m.addthisedge.com https://www.sc.pages05.net https://www.google-analytics.com https://sjs.bizographics.com https://static.ads-twitter.com https://*.pingdom.net https://snap.licdn.com https://vlog.leadformix.com https://*.facebook.com https://*.twitter.com https://www.google.com https://*.facebook.net https://*.linkedin.com https://*.adnxs.com https://players.brightcove.net https://vjs.zencdn.net https://www.fiserv.com blob: https://www.bizographics.com 'unsafe-inline' 'unsafe-eval'</td></tr>
<tr><td>csp_unsafe_policy</td><td>https://www.fiservdox.com/</td><td>https://www.fiservdox.com/</td><td>n/a</td><td>-</td><td>2019-01-29T09:10:53.470Z</td></tr>
<tr><td colspan="6">Evidence:
default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://ion.fiserv.com https://connect.facebook.net www.youtube.com https://players.brightcove.net https://hls.cf.brightcove.com https://fonts.gstatic.com https://fonts.googleapis.com https://cdn.hypemarks.com www.digitalfileshares.com https://brightcove.hs.llnwd.net www.fiserv.com https://www.fiserv.com https://vjs.zencdn.net https://www.google.ca https://*.addthis.com https://www.google.com https://secure.brightcove.com https://f1.media.brightcove.com data: https://metrics.brightcove.com https://edge.api.brightcove.com blob: https://*.doubleclick.net https://www.google.com https://8174811.fls.doubleclick.net https://www.google-analytics.com https://t.co https://stats.g.doubleclick.net https://vlog.leadformix.com https://www.facebook.com https://secure.adnxs.com https://www.pages05.net https://*.pingdom.net https://*.linkedin.com 'unsafe-inline' 'unsafe-eval'; script-src https://tagmanager.google.com https://ajax.googleapis.com https://8f2a3f802cdf2859af9e-51128641de34f0801c2bd5e1e5f0dc25.ssl.cf1.rackcdn.com https://api.keen.io https://www.fiserv.com https://s.ytimg.com https://www.youtube.com https://www.tintup.com https://*.cloudfront.net www.fiserv.com https://www.googletagmanager.com https://*.addthis.com https://m.addthisedge.com https://www.sc.pages05.net https://www.google-analytics.com</td></tr>
</table>

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

https://sjs.bizographics.com https://static.ads-twitter.com https://*.pingdom.net https://snap.licdn.com https://vlog.leadformix.com https://*.facebook.com https://*.twitter.com https://www.google.com https://*.facebook.net https://*.linkedin.com https://*.adnxs.com https://players.brightcove.net https://vjs.zencdn.net https://www.fiserv.com blob: https://www.bizographics.com 'unsafe-inline' 'unsafe-eval'					
csp_unsafe_policy	http://www.fiservdox.com/	http://www.fiservdox.com/	n/a	-	2019-01-29T09:10:53.412Z
Evidence: default-src https://ssl.gstatic.com https://www.gstatic.com https://cdnjs.cloudflare.com tagmanager.google.com https://ion.fiserv.com https://connect.facebook.net www.youtube.com https://players.brightcove.net https://hls.cf.brightcove.com https://fonts.gstatic.com https://fonts.googleapis.com https://cdn.hypemarks.com www.digitalfileshares.com https://brightcove.hs.llnwd.net www.fiserv.com https://www.fiserv.com https://vjs.zencdn.net https://www.google.ca https://*.addthis.com https://www.google.com https://secure.brightcove.com https://f1.media.brightcove.com data: https://metrics.brightcove.com https://edge.api.brightcove.com blob: https://*.doubleclick.net https://www.google.com https://8174811.fls.doubleclick.net https://www.google-analytics.com https://t.co https://stats.g.doubleclick.net https://vlog.leadformix.com https://www.facebook.com https://secure.adnxs.com https://www.pages05.net https://*.pingdom.net https://*.linkedin.com 'unsafe-inline' 'unsafe-eval'; script-src https://tagmanager.google.com https://ajax.googleapis.com https://8f2a3f802cdf2859af9e-51128641de34f0801c2bd5e1e5f0dc25.ssl.cf1.rackcdn.com https://api.keen.io https://www.fiserv.com https://s.ytimg.com https://www.youtube.com https://www.tintup.com https://*.cloudfront.net www.fiserv.com https://www.googletagmanager.com https://*.addthis.com https://m.addthisedge.com https://www.sc.pages05.net https://www.google-analytics.com https://sjs.bizographics.com https://static.ads-twitter.com https://*.pingdom.net https://snap.licdn.com https://vlog.leadformix.com https://*.facebook.com https://*.twitter.com https://www.google.com https://*.facebook.net https://*.linkedin.com https://*.adnxs.com https://players.brightcove.net https://vjs.zencdn.net https://www.fiserv.com blob: https://www.bizographics.com 'unsafe-inline' 'unsafe-eval'					
csp_unsafe_policy	https://sysadmin5-cert.fiserv.com/	https://sysadmin5-cert.fiserv.com/	n/a	-	2019-01-22T07:02:48.862Z
Evidence: default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; connect-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:; style-src 'self' 'unsafe-inline' 'unsafe-eval';					
csp_unsafe_policy	https://sysadmin5.fiserv.com/	https://sysadmin5.fiserv.com/	n/a	-	2019-01-22T07:02:45.601Z
Evidence: default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; connect-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:; style-src 'self' 'unsafe-inline' 'unsafe-eval';					
csp_unsafe_policy	https://sysadmin6-cert.fiserv.com/	https://sysadmin6-cert.fiserv.com/	n/a	-	2019-01-22T07:02:42.949Z
Evidence: default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; connect-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:; style-src 'self' 'unsafe-inline' 'unsafe-eval';					
csp_unsafe_policy	https://sysadmin6.fiserv.com/	https://sysadmin6.fiserv.com/	n/a	-	2019-01-22T07:02:41.175Z
Evidence: default-src 'none'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; connect-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:; style-src 'self' 'unsafe-inline' 'unsafe-eval';					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

RECOMMENDATION

Remove the unsafe directives from the content security policy. For trusted resources that must be used inline with HTML, you can use nonces or hashes in your content security policy's source list to mark the resources as trusted. Nonces are randomly generated numbers placed with inline content that you trust. By including the nonce in both the content and the header, the browser knows to trust the script. Example inline script with a nonce: <script nonce=aBFef03nceIOfn39hr3rsatsdfa>alert('Hello, world.');</script> Example policy that allows the inline script to be run without unsafe directives: Content-Security-Policy: script-src 'nonce-aBFef03nceIOfn39hr3rsatsdfa' Warning: For nonces to be effective, they must be randomly regenerated every time the page is loaded. If an attacker can guess the nonce value, the protection is useless. Hashes work similarly to nonces, but only need to be generated once. By taking the hash of a script and including it in the header, it will mark the script as trusted. If the attacker tries to change the script, the hash will change and it will no longer be trusted. Example inline script to be hashed: <script>alert('Hello, world.');</script> Example policy that allows the inline script to be run without unsafe directives: Content-Security-Policy: script-src 'sha256-qznLcsROx4GACP2dm0UCKCzCG-HiZ1guq6ZZDob_Tng='

ABOUT THIS ISSUE

The Content Security Policy (CSP) header can mitigate Cross-Site Scripting (XSS) attacks by prohibiting the browser from running code embedded within the HTML of your site. However, the use of unsafe-eval and unsafe-inline policies in the CSP prevent this key safety feature from functioning. These unsafe directives mean that, should the site be vulnerable to XSS or HTML injection attacks, the attacker will be able to inject their own resources directly into the HTML response and have the browser execute them.

APPLICATION SECURITY > ISSUE DETAIL

Website Does Not Implement HSTS Best Practices

Even if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website.

-1.0 SCORE IMPACT

85 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
no_hsts	https://staging.fiserv-ecomhosting.com/	https://staging.fiserv-ecomhosting.com/	n/a	No HSTS header found	2019-01-29T09:11:43.731Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://mail.fiservlendingsolutions.com/	https://mail.fiservlendingsolutions.com/	n/a	No HSTS header found	2019-01-29T09:11:17.099Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://webmail.fiserv.net/	https://webmail.fiserv.net/	n/a	No HSTS header found	2019-01-29T09:11:13.849Z
Evidence:					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

No Strict-Transport-Security header found.					
hsts_missing_subdomain	https://my.carreker.com/login.asp	https://my.carreker.com/	https://my.carreker.com/, 302, https://my.carreker.com/Login.asp	Header missing includeSubDomains directive	2019-01-29T09:10:59.822Z
Evidence: Strict-Transport-Security: max-age=157680000					
no_hsts	https://search.carreker.com/	https://search.carreker.com/	n/a	No HSTS header found	2019-01-29T09:10:57.094Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://careers.carreker.com/	https://careers.carreker.com/	n/a	No HSTS header found	2019-01-29T09:10:56.934Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://mail.billmatrix.com/	https://mail.billmatrix.com/	n/a	No HSTS header found	2019-01-29T09:10:56.928Z
Evidence: No Strict-Transport-Security header found.					
hsts_missing_subdomain	https://fiservdm.net/vpn/index.html	https://fiservdm.net/	https://fiservdm.net/, 302, https://fiservdm.net/vpn/index.html	Header missing includeSubDomains directive	2019-01-29T09:10:55.671Z
Evidence: Strict-Transport-Security: max-age=157680000					
hsts_missing_subdomain	https://support.fiservatlanta.net/	http://support.fiservatlanta.net/	http://support.fiservatlanta.net/, 302, https://support.fiservatlanta.net/	Header missing includeSubDomains directive	2019-01-29T09:10:54.014Z
Evidence: Strict-Transport-Security: max-age=31536000					
no_hsts	https://fiserv-ecomhosting.com/logon.asp	https://fiserv-ecomhosting.com/	https://fiserv-ecomhosting.com/, 302, https://fiserv-ecomhosting.com/logon.asp	No HSTS header found	2019-01-29T09:10:53.901Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://fiservwebsolutions.com/	https://fiservwebsolutions.com/	n/a	No HSTS header found	2019-01-29T09:10:53.876Z
Evidence: No Strict-Transport-Security header found.					
hsts_missing_subdomain	https://www.fiserv.com/customer-channel-management/output-solutions/operational-documents-supplies.aspx/	https://fiservdox.com/	https://fiservdox.com/, 302, https://www.fiserv.com/customer-channel-management/output-solutions/operational-documents-supplies.aspx/	Header missing includeSubDomains directive	2019-01-29T09:10:53.684Z
Evidence:					

Strict-Transport-Security: max-age=31536000					
no_hsts	https://www.fiserv-ecomhosting.com/logon.asp	http://www.fiserv-ecomhosting.com/	http://www.fiserv-ecomhosting.com/, 302, http://www.fiserv-ecomhosting.com/logon.asp, 302, https://www.fiserv-ecomhosting.com/logon.asp	No HSTS header found	2019-01-29T09:10:53.649Z
Evidence: No Strict-Transport-Security header found.					
hsts_missing_subdomain	https://www.fiservdox.com/	https://www.fiservdox.com/	n/a	Header missing includeSubDomains directive	2019-01-29T09:10:53.470Z
Evidence: Strict-Transport-Security: max-age=31536000					
no_hsts	https://alpha.hepsiian.com/	https://alpha.hepsiian.com/	n/a	No HSTS header found	2019-01-29T09:10:53.348Z
Evidence: No Strict-Transport-Security header found.					
hsts_missing_subdomain	https://auth01.client-central.com/nidp/idff/sso?requestid=idgngcjotbnf60kxgjik8ar7px-qm&majorversion=1&minorversion=2&issueinstant=2019-01-29t09%3a10%3a53z&providerid=https%3a%2f%2fwww.client-central.com%3a443%2fnesp%2fidff%2fmetadata&relaystate=ma%3d%3d&consent=urn%3aliberty%3aconsent%3aunavailable&agappna=clientcentral_home&forceauthn=false&ispassive=false&nameidpolicy=onetime&protocolprofile=http%3a%2f%2fprojectliberty.org%2fprofiles%2fbrws-art&target=https%3a%2f%2fwww.client-central.com%2f&authncontextstatementref=radius%2ftoken%2furi	http://secure.fiserveft.com/	http://secure.fiserveft.com/, 302, https://www.client-central.com/, 302, https://www.client-central.com:443/nesp/app/plogin?agAppNa=clientCentral_Home&c=radius/token/uri&target=%22https://www.client-central.com/%22, 302, https://auth01.client-central.com/nidp/idff/sso?RequestID=idGNGCJoTbNF60kxgjik8Ar7px-QM&MajorVersion=1&MinorVersion=2&IssueInstant=2019-01-29T09%3A10%3A53Z&ProviderID=https%3A%2F%2Fwww.client-central.com%3A443%2Fnesp%2Fidff%2Fmetadata&RelayState=MA%3D%3D&consent=urn%3Aliberty%3Aconsent%3Aunavailable&agAppNa=clientCentral_Home&ForceAuthn=false&IsPassive=false&NameIDPolicy=onetime&ProtocolProfile=http%3A%2F%2Fprojectliberty.org%2Fprofiles%2Fbrws-art&target=https%3A%2F%2Fwww.client-central.com%2F&Auth	Header missing includeSubDomains directive	2019-01-29T09:10:53.326Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

			nContextStatementRef=radius%2Ftoken%2Furi		
Evidence: Strict-Transport-Security: max-age=31536000					
no_hsts	https://images.hepsiian.com/	https://images.hepsiian.com/	n/a	No HSTS header found	2019-01-29T09:10:52.534Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://news.checkfree.com/	https://news.checkfree.com/	n/a	No HSTS header found	2019-01-29T09:10:52.427Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://www.fiservwebsolutions.com	http://fiservwebsolutions.com/	http://fiservwebsolutions.com/, 301, https://www.fiservwebsolutions.com	No HSTS header found	2019-01-29T09:10:52.406Z
Evidence: No Strict-Transport-Security header found.					
hsts_missing_subdomain	https://fiservsupport.com/	http://fiservsupport.com/	http://fiservsupport.com/, 302, https://fiservsupport.com/	Header missing includeSubDomains directive	2019-01-29T09:10:51.744Z
Evidence: Strict-Transport-Security: max-age=31536000					
no_hsts	https://fiservlendingsolutions.com/	https://fiservlendingsolutions.com/	n/a	No HSTS header found	2019-01-29T09:10:50.983Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://fiservipvpn.com/	https://fiservipvpn.com/	n/a	No HSTS header found	2019-01-29T09:10:50.584Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://www.fiservlendingsolutions.com/	https://www.fiservlendingsolutions.com/	n/a	No HSTS header found	2019-01-29T09:10:50.369Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://fiservcws.com/	https://fiservcws.com/	n/a	No HSTS header found	2019-01-29T09:10:50.069Z
Evidence: No Strict-Transport-Security header found.					
hsts_missing_subdomain	https://fiservdmdr.net/vpn/index.html	https://fiservdmdr.net/	https://fiservdmdr.net/, 302, https://fiservdmdr.net/vpn/index.html	Header missing includeSubDomains directive	2019-01-29T09:10:49.321Z
Evidence: Strict-Transport-Security: max-age=157680000					
no_hsts	https://www.careers.fiserv.com/	http://careers.fiserv.com/	http://careers.fiserv.com/, 301,	No HSTS header found	2019-01-29T09:09:27.681Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

			http://www.careers.fiserv.com, 301, https://www.careers.fiserv.com/		
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://alabama.fiservls.com/	https://alabama.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:16.824Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://en.fiservls.com/	https://en.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:16.760Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://blog.fiservls.com/	https://blog.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:16.759Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:16.742Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://shop.fiservls.com/	https://shop.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:16.731Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://bg.fiservls.com/	https://bg.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:16.726Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:16.715Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.968Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://in.fiservls.com/	https://in.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.961Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://ww.fiservls.com/	https://ww.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.955Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://espanol.fiservls	https://espanol.fiservls	n/a	No HSTS header	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	.com/	.com/		found	22T07:04:14.953Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://backend.fiservls.com/	https://backend.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.953Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://chat.fiservls.com/	https://chat.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.953Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://arizona.fiservls.com/	https://arizona.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.918Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://14.fiservls.com/	https://14.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.091Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.089Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://sadmin.fiservls.com/	https://sadmin.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.085Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://boston.fiservls.com/	https://boston.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.083Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://developer.fiservls.com/	https://developer.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.073Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://act.fiservls.com/	https://act.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.070Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://arlington.fiservls.com/	https://arlington.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.063Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://client.fiservls.com/	https://client.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.063Z
Evidence:					

No Strict-Transport-Security header found.					
no_hsts	https://ftp.fiservls.com/	https://ftp.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:14.047Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://blackberry.fiservls.com/	https://blackberry.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:13.296Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://citrix.fiservls.com/	https://citrix.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:13.214Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://arkansas.fiservls.com/	https://arkansas.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:13.209Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://biz.fiservls.com/	https://biz.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:13.207Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://survey.fiservls.com/	https://survey.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:12.891Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://demo.fiservls.com/	https://demo.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:12.891Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://au.fiservls.com/	https://au.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:12.849Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://team.fiservls.com/	https://team.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:03.075Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:03.053Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://ns1.fiservls.com/	https://ns1.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:03.005Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://131.fiservls.com	https://131.fiservls.com	n/a	No HSTS header	2019-01-

	/	/		found	22T07:04:02.976Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://forums.fiservls.com/	https://forums.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.940Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://corp.fiservls.com/	https://corp.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.904Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://apps.fiservls.com/	https://apps.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.857Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://atlanta.fiservls.com/	https://atlanta.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.851Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://customer.fiservls.com/	https://customer.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.784Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://intranet1.fiservls.com/	https://intranet1.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.756Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://18.fiservls.com/	https://18.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.716Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://administrador.fiservls.com/	https://administrador.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.681Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://backup.fiservls.com/	https://backup.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.590Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://apollo.fiservls.com/	https://apollo.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.577Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://manage.fiservls.com/	https://manage.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.496Z
Evidence:					

No Strict-Transport-Security header found.					
no_hsts	https://support.fiservls.com/	https://support.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.457Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://email.fiservls.com/	https://email.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.113Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://ad.fiservls.com/	https://ad.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.039Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://download.fiservls.com/	https://download.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:02.000Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://am.fiservls.com/	https://am.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:01.913Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://california.fiservls.com/	https://california.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:01.632Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://antivirus.fiservls.com/	https://antivirus.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:01.624Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://ajax.fiservls.com/	https://ajax.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:01.621Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://mail.fiservls.com/	https://mail.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:01.617Z
Evidence: No Strict-Transport-Security header found.					
no_hsts	https://pop.fiservls.com/	https://pop.fiservls.com/	n/a	No HSTS header found	2019-01-22T07:04:01.617Z
Evidence: No Strict-Transport-Security header found.					
hsts_missing_subdomain	https://sysadmin5-cert.fiserv.com/	https://sysadmin5-cert.fiserv.com/	n/a	Header missing includeSubDomains directive	2019-01-22T07:02:48.862Z
Evidence: Strict-Transport-Security: max-age=31536000					

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

hsts_missing_subdomain	https://sysadmin5.fiserv.com/	https://sysadmin5.fiserv.com/	n/a	Header missing includeSubDomains directive	2019-01-22T07:02:45.601Z
Evidence: Strict-Transport-Security: max-age=31536000					
hsts_missing_subdomain	https://sysadmin6-cert.fiserv.com/	https://sysadmin6-cert.fiserv.com/	n/a	Header missing includeSubDomains directive	2019-01-22T07:02:42.949Z
Evidence: Strict-Transport-Security: max-age=31536000					
hsts_missing_subdomain	https://sysadmin6.fiserv.com/	https://sysadmin6.fiserv.com/	n/a	Header missing includeSubDomains directive	2019-01-22T07:02:41.175Z
Evidence: Strict-Transport-Security: max-age=31536000					

RECOMMENDATION

Every web application (and any URLs traversed to arrive at the website via redirects) should set the HSTS header to remain in effect for at least 12 months (31536000 seconds). It is also recommended to set the 'includeSubDomains' directive so that requests to subdomains are also automatically upgraded to HTTPS. An acceptable HSTS header would declare: Strict-Transport-Security: max-age=31536000; includeSubDomains;

ABOUT THIS ISSUE

HTTP Strict Transport Security is an HTTP header that instructs clients (e.g., web browsers) to only connect to a website over encrypted HTTPS connections. Clients that respect this header will automatically upgrade all connection attempts from HTTP to HTTPS. After a client receives the HSTS header upon its first website visit, future connections to that website are protected against Man-in-the-Middle attacks that attempt to downgrade to an unencrypted HTTP connection. The browser will expire the HTTP Strict Transport Security header after the number of seconds configured in the max-age attribute.

APPLICATION SECURITY > ISSUE DETAIL

!!! Site does not enforce HTTPS

Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code).

-1.6 SCORE IMPACT

70 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
http_only	http://staging.fiserv-ecomhosting.com/	http://staging.fiserv-ecomhosting.com/	n/a	-	2019-01-29T09:11:43.673Z
http_only	http://services.fiserv-ecomhosting.com/	http://services.fiserv-ecomhosting.com/	n/a	-	2019-01-29T09:11:43.673Z
http_only	http://www.fiservsw.com/	http://www.fiservsw.com/	n/a	-	2019-01-29T09:11:42.823Z
http_only	http://fiservcreditservices.com/	http://fiservcreditservices.com/	n/a	-	2019-01-29T09:11:15.569Z
http_only	http://fiservsw.com/	http://fiservsw.com/	n/a	-	2019-01-29T09:11:05.384Z

http_only	http://search.carreker.com/	http://search.carreker.com/	n/a	-	2019-01-29T09:10:57.065Z
http_only	http://careers.carreker.com/	http://careers.carreker.com/	n/a	-	2019-01-29T09:10:56.855Z
http_only	http://agility-fiserv.com/	http://agility-fiserv.com/	n/a	-	2019-01-29T09:10:55.566Z
http_only	http://bbs.summitsite.com/	http://bbs.summitsite.com/	n/a	-	2019-01-29T09:10:53.790Z
http_only	http://www.fiservdox.com/	http://www.fiservdox.com/	n/a	-	2019-01-29T09:10:53.412Z
http_only	http://fiservlendingsolutions.com/	http://fiservlendingsolutions.com/	n/a	-	2019-01-29T09:10:50.913Z
http_only	http://demo.billmatrix.com/	http://demo.billmatrix.com/	n/a	-	2019-01-29T09:10:50.447Z
http_only	http://mail.fiservlendingsolutions.com/	http://mail.fiservlendingsolutions.com/	n/a	-	2019-01-29T09:10:50.349Z
http_only	http://www.fiservlendingsolutions.com/	http://www.fiservlendingsolutions.com/	n/a	-	2019-01-29T09:10:50.285Z
http_only	http://alabama.fiservls.com/	http://alabama.fiservls.com/	n/a	-	2019-01-22T07:04:16.763Z
http_only	http://en.fiservls.com/	http://en.fiservls.com/	n/a	-	2019-01-22T07:04:16.691Z
http_only	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	-	2019-01-22T07:04:16.691Z
http_only	http://blog.fiservls.com/	http://blog.fiservls.com/	n/a	-	2019-01-22T07:04:16.677Z
http_only	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	-	2019-01-22T07:04:16.662Z
http_only	http://shop.fiservls.com/	http://shop.fiservls.com/	n/a	-	2019-01-22T07:04:16.662Z
http_only	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	-	2019-01-22T07:04:16.646Z
http_only	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	-	2019-01-22T07:04:14.897Z
http_only	http://download.fiservls.com/	http://download.fiservls.com/	n/a	-	2019-01-22T07:04:14.897Z
http_only	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	-	2019-01-22T07:04:14.897Z
http_only	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	-	2019-01-22T07:04:14.897Z
http_only	http://backend.fiservls.com/	http://backend.fiservls.com/	n/a	-	2019-01-22T07:04:14.878Z
http_only	http://in.fiservls.com/	http://in.fiservls.com/	n/a	-	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

					22T07:04:14.878Z
http_only	http://espanol.fiservls.com/	http://espanol.fiservls.com/	n/a	-	2019-01-22T07:04:14.863Z
http_only	http://forums.fiservls.com/	http://forums.fiservls.com/	n/a	-	2019-01-22T07:04:14.853Z
http_only	http://arizona.fiservls.com/	http://arizona.fiservls.com/	n/a	-	2019-01-22T07:04:14.849Z
http_only	http://chat.fiservls.com/	http://chat.fiservls.com/	n/a	-	2019-01-22T07:04:14.849Z
http_only	http://mobile.fiservls.com/	http://mobile.fiservls.com/	n/a	-	2019-01-22T07:04:14.017Z
http_only	http://14.fiservls.com/	http://14.fiservls.com/	n/a	-	2019-01-22T07:04:14.016Z
http_only	http://boston.fiservls.com/	http://boston.fiservls.com/	n/a	-	2019-01-22T07:04:14.015Z
http_only	http://sadmin.fiservls.com/	http://sadmin.fiservls.com/	n/a	-	2019-01-22T07:04:14.014Z
http_only	http://developer.fiservls.com/	http://developer.fiservls.com/	n/a	-	2019-01-22T07:04:13.993Z
http_only	http://act.fiservls.com/	http://act.fiservls.com/	n/a	-	2019-01-22T07:04:13.993Z
http_only	http://client.fiservls.com/	http://client.fiservls.com/	n/a	-	2019-01-22T07:04:13.990Z
http_only	http://backup.fiservls.com/	http://backup.fiservls.com/	n/a	-	2019-01-22T07:04:13.984Z
http_only	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	-	2019-01-22T07:04:13.780Z
http_only	http://citrix.fiservls.com/	http://citrix.fiservls.com/	n/a	-	2019-01-22T07:04:13.145Z
http_only	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	-	2019-01-22T07:04:13.145Z
http_only	http://blackberry.fiservls.com/	http://blackberry.fiservls.com/	n/a	-	2019-01-22T07:04:13.145Z
http_only	http://arkansas.fiservls.com/	http://arkansas.fiservls.com/	n/a	-	2019-01-22T07:04:13.145Z
http_only	http://demo.fiservls.com/	http://demo.fiservls.com/	n/a	-	2019-01-22T07:04:12.815Z
http_only	http://survey.fiservls.com/	http://survey.fiservls.com/	n/a	-	2019-01-22T07:04:12.815Z
http_only	http://arlington.fiservls.com/	http://arlington.fiservls.com/	n/a	-	2019-01-22T07:04:05.405Z
http_only	http://fiservdox.com/	http://fiservdox.com/	n/a	-	2019-01-22T07:04:03.821Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

http_only	http://mail.fiservls.com/	http://mail.fiservls.com/	n/a	-	2019-01-22T07:04:03.030Z
http_only	http://team.fiservls.com/	http://team.fiservls.com/	n/a	-	2019-01-22T07:04:03.013Z
http_only	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	-	2019-01-22T07:04:02.968Z
http_only	http://pop.fiservls.com/	http://pop.fiservls.com/	n/a	-	2019-01-22T07:04:02.920Z
http_only	http://131.fiservls.com/	http://131.fiservls.com/	n/a	-	2019-01-22T07:04:02.897Z
http_only	http://corp.fiservls.com/	http://corp.fiservls.com/	n/a	-	2019-01-22T07:04:02.819Z
http_only	http://apps.fiservls.com/	http://apps.fiservls.com/	n/a	-	2019-01-22T07:04:02.789Z
http_only	http://atlanta.fiservls.com/	http://atlanta.fiservls.com/	n/a	-	2019-01-22T07:04:02.748Z
http_only	http://customer.fiservls.com/	http://customer.fiservls.com/	n/a	-	2019-01-22T07:04:02.710Z
http_only	http://intranet1.fiservls.com/	http://intranet1.fiservls.com/	n/a	-	2019-01-22T07:04:02.673Z
http_only	http://18.fiservls.com/	http://18.fiservls.com/	n/a	-	2019-01-22T07:04:02.638Z
http_only	http://administrador.fiservls.com/	http://administrador.fiservls.com/	n/a	-	2019-01-22T07:04:02.606Z
http_only	http://apollo.fiservls.com/	http://apollo.fiservls.com/	n/a	-	2019-01-22T07:04:02.487Z
http_only	http://manage.fiservls.com/	http://manage.fiservls.com/	n/a	-	2019-01-22T07:04:02.415Z
http_only	http://au.fiservls.com/	http://au.fiservls.com/	n/a	-	2019-01-22T07:04:02.382Z
http_only	http://support.fiservls.com/	http://support.fiservls.com/	n/a	-	2019-01-22T07:04:02.382Z
http_only	http://email.fiservls.com/	http://email.fiservls.com/	n/a	-	2019-01-22T07:04:02.030Z
http_only	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	-	2019-01-22T07:04:01.957Z
http_only	http://am.fiservls.com/	http://am.fiservls.com/	n/a	-	2019-01-22T07:04:01.824Z
http_only	http://antivirus.fiservls.com/	http://antivirus.fiservls.com/	n/a	-	2019-01-22T07:04:01.560Z
http_only	http://california.fiservls.com/	http://california.fiservls.com/	n/a	-	2019-01-22T07:04:01.560Z
http_only	http://ajax.fiservls.com	http://ajax.fiservls.com	n/a	-	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	/	/			22T07:04:01.560Z

RECOMMENDATION

Any site served to a user (possibly at the end of a redirect chain) should be served over HTTPS.

ABOUT THIS ISSUE

The site responds to HTTP requests without ultimately redirecting the browser to a secure version of the page. Since the site allows plaintext traffic, a man-in-the-middle attacker is able to read and modify any information passed between the site and the user. There are a variety of situations in which an attacker can intercept plaintext traffic in a man-in-the-middle position, including but not limited to: * Open Wi-Fi Hotspots * WPA/WPA2 encrypted hot-spots where the attacker connected before the victim * Malicious Wi-Fi access points * Compromised switches and routers * ARP poisoning on the same wired network It's important to remember that in many of the above situations, an attacker can not only read traffic, but also actively modify the traffic. Even if a site that does not contain sensitive information, an attacker can still inject malicious content to a user's browser.

APPLICATION SECURITY > ISSUE DETAIL

‼ Insecure HTTPS Redirect Pattern

Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site.

-0.9 SCORE IMPACT

6 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
https_redirect_different_apex	https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3a%2f%2flogin.microsoftonline.com%2fte%2ffiservservicepoint.onmicrosoft.com%2fb2c_1a_prod_sn_signin%2fsamlp%2fsso%2flogin%3fsamlrequest%3dlvlbbptaep0vthdgoxfjvsyssvxvupki2o2hf2sdg7mszjcdhsr%252fx8akts%252bwep15896bn7ni3drxq7lopeedphfaznttamr17qsis6his2gfugfwrld77o5wxyfursvhbdxcy5jboko4iesuabsh25scfj7cpuljuzzvgfzmapubn1s%252b0ktquboi7lt9gqak4w0hawb1ypr3rqatwaaxhswmyhhwbmeadtctzpwtgxqb4qd2qt3em2ouhxnl	http://my.carreker.com/	http://my.carreker.com/, 302, https://c3.fiserv.com/, 302, https://servicepoint.fiservapps.com/, 302, https://fiserv.service-now.com/, 302, https://fiserv.service-now.com/auth_redirect.do?sysparm_url=https%3A%2F%2Flogin.microsoftonline.com%2Fte%2Ffiservservicepoint.onmicrosoft.com%2FB2C_1A_Prod_sn_signin%2Fsamlp%2Fsso%2Flogin%3FSAMLRequest%3DlVLBbptAEP0VtHdgoXFjVsYSsVXVUpKi2O2hF2sDg7MSzJCdhSR%252FX8AkTS%252BWep15896bN7Ni3dRxq7LOPeEDPHfAzn	Redirect goes to different apex domain	2019-01-29T09:11:00.692Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	5zhxyoaebsnxwtzkpjo%252f8l6rlwbkihwvrhmet9umyn%252b%252fwzz6uutfnxyvchlheqrf4ssyizfy%252buqxquqa5fwzmx5s4ww3tjj3sen2gl0qyhklvoz8odnirewrkjk4sulfwsvncg8mlgzpl%252fn%252bpinyft8ccj%252f%252fst9mbl0pwd4p6p%252bk%252bhdynmiemmv6nd1btbbt5xe47ei%252f312sl0uvws8cs1yrrte7bu61kd68rk7pzwnbu48yh5s02l32mfzm6vctvlxjwuwanqjxs%252bq%252fd77%252baw%253d%253d%26relaystate%3dhttps%253a%252f%252ffiserv.service-now.com%252fnavpage.do		ttamR17qSis6hls2GFugFWrlD77O5WxYFUrSVHBdXCy5jBOkO4IeSuAbsH25sCfj7cpuLJuZZVGFZmAPUBn1s%252B0ktQUBOi7lt9gqAk4W0HAwb1yPR3rqaTwaAxhSWmyhHWBmEadTCTzpwtGXQB4Qd2Qt3Em2OUHXNL5ZHxyOaEBsNxwTZkpjO%252F8L6RLWBKIhWVrhmEt9umYn%252B%252FWZZ6UUTFNXyVchlHEqrF4ssyiZfy%252BuqxquQA5Fwzmx5S4Ww3TjJ3sEN2Gl0qYhklvoz8ODnIREWRkjK4SuLfwsvnCG8MlgZPl%252FN%252BPINYfT8ccj%252F%252FsT9MBL0pwd4P6P%252BK%252BhdYnmIemMV6Nd1bTbbt5xe47Ei%252F312sL0uvws8Cs1yrRte7bU61Kd68rK7pZWNBu48Yh5s02l32MFZM6VcTVLXjWuwAnQjXs%252Bq%252FD77%252BAw%253D%253D%26RelayState%3Dhttps%253A%252F%252Ffiserv.service-now.com%252Fnavpage.do		
https_redirect_different_apex	https://www.fiserv.com/index.aspx	http://www.summitsite.com/	http://www.summitsite.com/, 301, https://www.fiserv.com, 301, https://www.fiserv.com/index.aspx	Redirect goes to different apex domain	2019-01-29T09:10:54.588Z
Evidence: Strict-Transport-Security: max-age=31536000					
https_redirect_different_apex	https://auth01.client-central.com/nidp/idff/sso?requestid=idjrjdyv6vzonct0nte5k88oirdqi&majorversion=1&minorversion=2&issueinstant=2019-01-29t09%3a10%3a52z&providerid=https%3a%2f%2fwww.client-central.com%3a443%2fnesp%2fidff%2fmetadata&relaystate=ma%3d%3d&consent=urn%3aliberty%3aconsent%3aunavailable&agappna=clientcentral_home&forceauthn=false&ispassive=false&na	http://www.fiserveft.com/	http://www.fiserveft.com/, 302, https://www.client-central.com/, 302, https://www.client-central.com:443/nesp/app/plogin?agAppNa=clientCentral_Home&c=radius/token/uri&target=%22https://www.client-central.com/%22, 302, https://auth01.client-central.com/nidp/idff/sso?RequestID=idJrJDYV6VZoncT0nte5K88OIRdqI&MajorVersion=1&MinorVersion=2&IssueInstant=2019-01-	Redirect goes to different apex domain	2019-01-29T09:10:53.040Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

	meidpolicy=onetime&protocolprofile=http%3a%2f%2fprojectliberty.org%2fprofiles%2fbrws-art&target=https%3a%2f%2fwww.client-central.com%2f&authncontextstatementref=radius%2ftoken%2furi		29T09%3A10%3A52Z&ProviderID=https%3A%2F%2Fwww.client-central.com%3A443%2Fnesp%2Fidff%2Fmetadata&RelayState=MA%3D%3D&consent=urn%3Aliberty%3Aconsent%3Aunavailable&agAppNa=clientCentral_Home&ForceAuthn=false&IsPassive=false&NameIDPolicy=onetime&ProtocolProfile=http%3A%2F%2Fprojectliberty.org%2Fprofiles%2Fbrws-art&target=https%3A%2F%2Fwww.client-central.com%2F&AuthnContextStatementRef=radius%2Ftoken%2Furi		
Evidence: Strict-Transport-Security: max-age=31536000;includeSubDomains					
https_redirect_add_subdomain	https://www.fiservwebsolutions.com	http://fiservwebsolutions.com/	http://fiservwebsolutions.com/, 301, https://www.fiservwebsolutions.com	Redirect goes to a different subdomain	2019-01-29T09:10:52.406Z
https_redirect_add_subdomain	https://www.fiserv.com/index.aspx	http://fiserv.com/	http://fiserv.com/, 302, https://www.fiserv.com/, 301, https://www.fiserv.com/index.aspx	Redirect goes to a different subdomain	2019-01-29T09:09:40.297Z
Evidence: Strict-Transport-Security: max-age=31536000					
https_redirect_hsts_header_missing_includesubdomains	https://www.fiserv.com/index.aspx	http://test.fiserv.com/	http://test.fiserv.com/, 301, https://www.fiserv.com, 301, https://www.fiserv.com/index.aspx	HSTS header missing includeSubDomains directive	2019-01-29T09:09:29.254Z
Evidence: Strict-Transport-Security: max-age=31536000					

RECOMMENDATION

Any HTTP site should redirect the user to a secure (i.e. HTTPS) version of the same domain that was originally requested (or a higher-level/parent version of that same domain). For example, http://www.example.com should only redirect either to https://www.example.com or https://example.com. This redirect should be done before redirecting to any other domain or subdomain.

ABOUT THIS ISSUE

The HTTP site redirects users to a new URL in a way that cannot be secured with HTTPS and HSTS headers. This leaves users open to man-in-the-middle attackers who can redirect them to a fraudulent/ spoofed version of the intended site. Please see “Site Does Not Enforce HTTPS” issue type for more information regarding man-in-the-middle scenarios.

APPLICATION SECURITY > ISSUE DETAIL

Redirect Chain Contains HTTP

Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site.

-0.9 SCORE IMPACT

4 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
redirect_chain_contains_http	https://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx	http://www.fiserv-galaxy.com/	http://www.fiserv-galaxy.com/, 302, http://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx, 302, https://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx	Redirect chain contains an HTTP destination	2019-01-29T09:10:53.696Z
redirect_chain_contains_http	https://www.fiserv-ecomhosting.com/logon.asp	http://www.fiserv-ecomhosting.com/	http://www.fiserv-ecomhosting.com/, 302, http://www.fiserv-ecomhosting.com/logon.asp, 302, https://www.fiserv-ecomhosting.com/logon.asp	Redirect chain contains an HTTP destination	2019-01-29T09:10:53.649Z
redirect_chain_contains_http	https://www.careers.fiserv.com/	https://careers.fiserv.com/	https://careers.fiserv.com/, 301, http://www.careers.fiserv.com, 301, https://www.careers.fiserv.com/	Redirect chain contains an HTTP destination	2019-01-29T09:09:27.681Z
redirect_chain_contains_http	https://fiservsupport.com/	http://www.fiservsupport.com/	http://www.fiservsupport.com/, 302, http://fiservsupport.com/, 302, https://fiservsupport.com/	Redirect chain contains an HTTP destination	2019-01-22T07:04:04.073Z

RECOMMENDATION

Any HTTP site should immediately redirect users to HTTPS-protected URLs and ensure that any further redirects do not occur over HTTP. Prefer the usage of HTTPS URLs over HTTP when available, avoiding an unnecessary redirect.

ABOUT THIS ISSUE

While redirecting a user to their ultimate URL destination, the user passes through one or more URLs served over HTTP (instead of HTTPS). Having HTTP links in a redirect chain weakens other security technologies (e.g., HTTPS and HSTS headers) that are deployed elsewhere in the chain.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

APPLICATION SECURITY > ISSUE DETAIL

Unsafe Implementation Of Subresource Integrity

Subresource integrity (SRI) is a security feature that enables browsers to verify that files they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing website elements to provide a cryptographic hash that a fetched file must match.

7 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
sri_not_implemented	http://agility-fiserv.com/	http://agility-fiserv.com/	n/a	-	2019-01-29T09:10:55.566Z
Evidence: <script src="https://www.sc.pages05.net/lp/static/js/iMAWebCookie.js?3859023a-142e3c17146-c6f842ded9e6d11c5ffebd715e129037&h=www.pages05.net" type="text/javascript">					
sri_not_implemented	http://bbs.summitsite.com/	http://bbs.summitsite.com/	n/a	-	2019-01-29T09:10:53.790Z
Evidence: <script src="https://www.sc.pages05.net/lp/static/js/iMAWebCookie.js?3859023a-142e3c17146-c6f842ded9e6d11c5ffebd715e129037&h=www.pages05.net" type="text/javascript">					
sri_not_implemented	https://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx	https://www.fiserv-galaxy.com/	https://www.fiserv-galaxy.com/, 302, http://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx, 302, https://www.fiserv.com/industries/credit-unions/account-processing-platforms/galaxy.aspx	-	2019-01-29T09:10:53.771Z
Evidence: <script src="https://www.sc.pages05.net/lp/static/js/iMAWebCookie.js?3859023a-142e3c17146-c6f842ded9e6d11c5ffebd715e129037&h=www.pages05.net" type="text/javascript">,<script type="text/javascript" src="//s7.addthis.com/js/300/addthis_widget.js#pubid=ra-58beb6aeb83e506c">					
sri_not_implemented	https://www.fiservdox.com/	https://www.fiservdox.com/	n/a	-	2019-01-29T09:10:53.470Z
Evidence: <script src="https://www.sc.pages05.net/lp/static/js/iMAWebCookie.js?3859023a-142e3c17146-c6f842ded9e6d11c5ffebd715e129037&h=www.pages05.net" type="text/javascript">					
sri_not_implemented	http://www.fiservdox.com/	http://www.fiservdox.com/	n/a	-	2019-01-29T09:10:53.412Z
Evidence: <script src="https://www.sc.pages05.net/lp/static/js/iMAWebCookie.js?3859023a-142e3c17146-c6f842ded9e6d11c5ffebd715e129037&h=www.pages05.net" type="text/javascript">					
sri_not_implemented	https://www.fiservwebsolutions.com	http://fiservwebsolutions.com/	http://fiservwebsolutions.com/, 301, https://www.fiservwebsolutions.com	-	2019-01-29T09:10:52.406Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Evidence:
<link rel='stylesheet' id='google-fonts-css' href='//fonts.googleapis.com/css?family=Open+Sans%3A400%2C400italic%2C300italic%2C300%2C600%2C600italic%7CLato%3A400%2C100%2C300%2C700%7CJosefin+Slab%3A400%2C100%2C100italic%2C300%2C300italic%2C400italic%2C600%2C600italic%2C700%2C700italic%7CRoboto%3A400%2C100%2C100italic%2C300%2C300italic%2C400italic%2C500%2C500italic%2C700italic%2C700%2C900%2C900italic&#038;ver=4.7.10' type='text/css' media='all' />,<script type='text/javascript' src='//maps.googleapis.com/maps/api/js?v=3.exp%3Fsensor%3Dfalse&#038;ver=3.0'>

sri_not_implemented	https://www.careers.fiserv.com/	https://careers.fiserv.com/	https://careers.fiserv.com/, 301, http://www.careers.fiserv.com, 301, https://www.careers.fiserv.com/	-	2019-01-29T09:09:27.681Z

Evidence:
<link rel="stylesheet" type="text/css" href="//tbcdn.talentbrew.com/company/1758/v1/js/slick.css"/>,<link rel="stylesheet" href="//tbcdn.talentbrew.com/company/1758/css/4471-Full.css"/>,<link rel="stylesheet" type="text/css" href="http://localhost/fiserv/company/tb/css/style.css">,<script src="//tbcdn.talentbrew.com/js/client/adframe.js">,<script src="//players.brightcove.net/2474524878001/default_default/index.min.js">,<script src="//players.brightcove.net/2474524878001/default_default/index.min.js">,<script src="//tbcdn.talentbrew.com/bundles/tb-core">,<script src="//tbcdn.talentbrew.com/company/1758/v1/js/slick.min.js">,<script src="//use.fontawesome.com/bb4a8a1a47.js">,<script src="//tbcdn.talentbrew.com/company/1758/js/4471-Full.min.js">,<script src="//tbcdn.talentbrew.com/bundles/form">,<script id="tmp-magic-bullet" src="https://services.tmpwebeng.com/magicbullet/" data-gdpr="true" data-gdpr-policy-url="https://www.fiserv.com/about/privacypolicy.aspx" data-gdpr-client-name="Fiserv">

RECOMMENDATION

Please ensure that all website elements (i.e. <script> and <link>) loading JavaScript and CSS stylesheets hosted with external organizations contain the 'integrity' directive with a valid checksum. Example: <script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>

ABOUT THIS ISSUE

Many websites that rely on JavaScript and CSS stylesheet files will host these static resources with external organizations (typically CDNs) to improve website load times. Unfortunately, if one of these external organizations is compromised then the JavaScript and CSS files it hosts can also be compromised and used to push malicious code to the original website. Subresource integrity is a way for a website owner to add a checksum value to all externally-hosted files that is used by the browser to verify that files loaded from external organizations have not been modified.

APPLICATION SECURITY > ISSUE DETAIL

‼ Website does not implement X-Frame-Options Best Practices

Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks.

-0.9 SCORE IMPACT

143 findings

ANALYSIS	FINAL URL	INITIAL URL	REQUEST CHAIN	ANALYSIS DESCRIPTION	LAST SEEN
x_frame_options_missing	https://staging.fiserv-ecomhosting.com/	https://staging.fiserv-ecomhosting.com/	n/a	Header missing	2019-01-29T09:11:43.731Z
x_frame_options_missing	http://staging.fiserv-ecomhosting.com/	http://staging.fiserv-ecomhosting.com/	n/a	Header missing	2019-01-29T09:11:43.673Z
x_frame_options_missing	http://www.fiservsw.com/	http://www.fiservsw.com/	n/a	Header missing	2019-01-29T09:11:42.823Z
x_frame_options_missing	https://mail.fiservlendingsolutions.com/	https://mail.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:11:17.099Z

x_frame_options_missing	http://fiservcreditservices.com/	http://fiservcreditservices.com/	n/a	Header missing	2019-01-29T09:11:15.569Z
x_frame_options_missing	https://webmail.fiserv.net/	https://webmail.fiserv.net/	n/a	Header missing	2019-01-29T09:11:13.849Z
x_frame_options_missing	http://fiservsw.com/	http://fiservsw.com/	n/a	Header missing	2019-01-29T09:11:05.384Z
x_frame_options_missing	https://my.carreker.com/login.asp	https://my.carreker.com/	https://my.carreker.com/, 302, https://my.carreker.com/Login.asp	Header missing	2019-01-29T09:10:59.822Z
x_frame_options_missing	https://search.carreker.com/	https://search.carreker.com/	n/a	Header missing	2019-01-29T09:10:57.094Z
x_frame_options_missing	http://search.carreker.com/	http://search.carreker.com/	n/a	Header missing	2019-01-29T09:10:57.065Z
x_frame_options_missing	https://careers.carreker.com/	https://careers.carreker.com/	n/a	Header missing	2019-01-29T09:10:56.934Z
x_frame_options_missing	https://mail.billmatrix.com/	https://mail.billmatrix.com/	n/a	Header missing	2019-01-29T09:10:56.928Z
x_frame_options_missing	http://careers.carreker.com/	http://careers.carreker.com/	n/a	Header missing	2019-01-29T09:10:56.855Z
x_frame_options_multiple	https://fiservdm.net/vpn/index.html	https://fiservdm.net/	https://fiservdm.net/, 302, https://fiservdm.net/vpn/index.html	Multiple headers found	2019-01-29T09:10:55.671Z
Evidence: X-Frame-Options: SAMEORIGIN,X-Frame-Options: SAMEORIGIN					
x_frame_options_missing	https://support.fiservatlanta.net/	http://support.fiservatlanta.net/	http://support.fiservatlanta.net/, 302, https://support.fiservatlanta.net/	Header missing	2019-01-29T09:10:54.014Z
x_frame_options_missing	https://fiserv-ecomhosting.com/logon.asp	https://fiserv-ecomhosting.com/	https://fiserv-ecomhosting.com/, 302, https://fiserv-ecomhosting.com/logon.asp	Header missing	2019-01-29T09:10:53.901Z
x_frame_options_missing	https://fiservwebsolutions.com/	https://fiservwebsolutions.com/	n/a	Header missing	2019-01-29T09:10:53.876Z
x_frame_options_missing	https://www.fiserv-ecomhosting.com/logon.asp	http://www.fiserv-ecomhosting.com/	http://www.fiserv-ecomhosting.com/, 302, http://www.fiserv-ecomhosting.com/logon.asp, 302, https://www.fiserv-ecomhosting.com/logon.asp	Header missing	2019-01-29T09:10:53.649Z
x_frame_options_missing	https://alpha.hepsiian.com/	https://alpha.hepsiian.com/	n/a	Header missing	2019-01-29T09:10:53.348Z
x_frame_options_missing	https://images.hepsiian.com/	https://images.hepsiian.com/	n/a	Header missing	2019-01-29T09:10:52.534Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_frame_options_missing	https://fiservsupport.com/	http://fiservsupport.com/	http://fiservsupport.com/, 302, https://fiservsupport.com/	Header missing	2019-01-29T09:10:51.744Z
x_frame_options_missing	https://fiservlendingsolutions.com/	https://fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.983Z
x_frame_options_missing	http://fiservlendingsolutions.com/	http://fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.913Z
x_frame_options_missing	https://fiservipvpn.com/	https://fiservipvpn.com/	n/a	Header missing	2019-01-29T09:10:50.584Z
x_frame_options_missing	http://demo.billmatrix.com/	http://demo.billmatrix.com/	n/a	Header missing	2019-01-29T09:10:50.447Z
x_frame_options_missing	https://www.fiservlendingsolutions.com/	https://www.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.369Z
x_frame_options_missing	http://mail.fiservlendingsolutions.com/	http://mail.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.349Z
x_frame_options_missing	http://www.fiservlendingsolutions.com/	http://www.fiservlendingsolutions.com/	n/a	Header missing	2019-01-29T09:10:50.285Z
x_frame_options_missing	https://fiservcws.com/	https://fiservcws.com/	n/a	Header missing	2019-01-29T09:10:50.069Z
x_frame_options_multiple	https://fiservdmdr.net/vpn/index.html	https://fiservdmdr.net/	https://fiservdmdr.net/, 302, https://fiservdmdr.net/vpn/index.html	Multiple headers found	2019-01-29T09:10:49.321Z
Evidence: X-Frame-Options: SAMEORIGIN,X-Frame-Options: SAMEORIGIN					
x_frame_options_missing	https://www.careers.fiserv.com/	https://careers.fiserv.com/	https://careers.fiserv.com/, 301, http://www.careers.fiserv.com, 301, https://www.careers.fiserv.com/	Header missing	2019-01-29T09:09:27.681Z
x_frame_options_missing	https://alabama.fiservls.com/	https://alabama.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.824Z
x_frame_options_missing	http://alabama.fiservls.com/	http://alabama.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.763Z
x_frame_options_missing	https://en.fiservls.com/	https://en.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.760Z
x_frame_options_missing	https://blog.fiservls.com/	https://blog.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.759Z
x_frame_options_missing	https://ca.fiservls.com/	https://ca.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.742Z
x_frame_options_missing	https://shop.fiservls.com/	https://shop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.731Z
x_frame_options_missing	https://bg.fiservls.com/	https://bg.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.726Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_frame_options_missing	https://bf.fiservls.com/	https://bf.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.715Z
x_frame_options_missing	http://ca.fiservls.com/	http://ca.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.691Z
x_frame_options_missing	http://en.fiservls.com/	http://en.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.691Z
x_frame_options_missing	http://blog.fiservls.com/	http://blog.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.677Z
x_frame_options_missing	http://shop.fiservls.com/	http://shop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.662Z
x_frame_options_missing	http://bg.fiservls.com/	http://bg.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.662Z
x_frame_options_missing	http://bf.fiservls.com/	http://bf.fiservls.com/	n/a	Header missing	2019-01-22T07:04:16.646Z
x_frame_options_missing	https://ap.fiservls.com/	https://ap.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.968Z
x_frame_options_missing	https://in.fiservls.com/	https://in.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.961Z
x_frame_options_missing	https://ww.fiservls.com/	https://ww.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.955Z
x_frame_options_missing	https://chat.fiservls.com/	https://chat.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z
x_frame_options_missing	https://backend.fiservls.com/	https://backend.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z
x_frame_options_missing	https://espanol.fiservls.com/	https://espanol.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.953Z
x_frame_options_missing	https://arizona.fiservls.com/	https://arizona.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.918Z
x_frame_options_missing	http://ap.fiservls.com/	http://ap.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_frame_options_missing	http://ns1.fiservls.com/	http://ns1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_frame_options_missing	http://download.fiservls.com/	http://download.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_frame_options_missing	http://ww.fiservls.com/	http://ww.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.897Z
x_frame_options_missing	http://backend.fiservls.com/	http://backend.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.878Z
x_frame_options_missing	http://in.fiservls.com/	http://in.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.878Z
x_frame_options_missing	http://espanol.fiservls.com/	http://espanol.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.863Z
x_frame_options_missing	http://forums.fiservls.com/	http://forums.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.853Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_frame_options_missing	http://arizona.fiservls.com/	http://arizona.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.849Z
x_frame_options_missing	http://chat.fiservls.com/	http://chat.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.849Z
x_frame_options_missing	https://14.fiservls.com/	https://14.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.091Z
x_frame_options_missing	https://mobile.fiservls.com/	https://mobile.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.089Z
x_frame_options_missing	https://sadmin.fiservls.com/	https://sadmin.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.085Z
x_frame_options_missing	https://boston.fiservls.com/	https://boston.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.083Z
x_frame_options_missing	https://developer.fiservls.com/	https://developer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.073Z
x_frame_options_missing	https://act.fiservls.com/	https://act.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.070Z
x_frame_options_missing	https://client.fiservls.com/	https://client.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.063Z
x_frame_options_missing	https://arlington.fiservls.com/	https://arlington.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.063Z
x_frame_options_missing	https://ftp.fiservls.com/	https://ftp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.047Z
x_frame_options_missing	http://mobile.fiservls.com/	http://mobile.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.017Z
x_frame_options_missing	http://14.fiservls.com/	http://14.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.016Z
x_frame_options_missing	http://boston.fiservls.com/	http://boston.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.015Z
x_frame_options_missing	http://sadmin.fiservls.com/	http://sadmin.fiservls.com/	n/a	Header missing	2019-01-22T07:04:14.014Z
x_frame_options_missing	http://developer.fiservls.com/	http://developer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.993Z
x_frame_options_missing	http://act.fiservls.com/	http://act.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.993Z
x_frame_options_missing	http://client.fiservls.com/	http://client.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.990Z
x_frame_options_missing	http://backup.fiservls.com/	http://backup.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.984Z
x_frame_options_missing	http://ftp.fiservls.com/	http://ftp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.780Z
x_frame_options_missing	https://blackberry.fiservls.com/	https://blackberry.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.296Z
x_frame_options_mis	https://citrix.fiservls.co	https://citrix.fiservls.co	n/a	Header missing	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

sing	m/	m/			22T07:04:13.214Z
x_frame_options_missing	https://arkansas.fiservls.com/	https://arkansas.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.209Z
x_frame_options_missing	https://biz.fiservls.com/	https://biz.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.207Z
x_frame_options_missing	http://citrix.fiservls.com/	http://citrix.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_frame_options_missing	http://blackberry.fiservls.com/	http://blackberry.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_frame_options_missing	http://biz.fiservls.com/	http://biz.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_frame_options_missing	http://arkansas.fiservls.com/	http://arkansas.fiservls.com/	n/a	Header missing	2019-01-22T07:04:13.145Z
x_frame_options_missing	https://demo.fiservls.com/	https://demo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.891Z
x_frame_options_missing	https://survey.fiservls.com/	https://survey.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.891Z
x_frame_options_missing	https://au.fiservls.com/	https://au.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.849Z
x_frame_options_missing	http://survey.fiservls.com/	http://survey.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.815Z
x_frame_options_missing	http://demo.fiservls.com/	http://demo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:12.815Z
x_frame_options_multiple	https://flagstar-devicemanager-uat.fiservapps.com/	https://flagstar-devicemanager-uat.fiservapps.com/	n/a	Multiple headers found	2019-01-22T07:04:09.273Z
Evidence: X-Frame-Options: DENY,X-Frame-Options: sameorigin					
x_frame_options_missing	http://arlington.fiservls.com/	http://arlington.fiservls.com/	n/a	Header missing	2019-01-22T07:04:05.405Z
x_frame_options_missing	http://fiservdox.com/	http://fiservdox.com/	n/a	Header missing	2019-01-22T07:04:03.821Z
x_frame_options_missing	https://team.fiservls.com/	https://team.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.075Z
x_frame_options_missing	https://ac.fiservls.com/	https://ac.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.053Z
x_frame_options_missing	http://mail.fiservls.com/	http://mail.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.030Z
x_frame_options_missing	http://team.fiservls.com/	http://team.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.013Z
x_frame_options_missing	https://ns1.fiservls.com/	https://ns1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:03.005Z
x_frame_options_missing	https://131.fiservls.com/	https://131.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.976Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

x_frame_options_missing	http://ac.fiservls.com/	http://ac.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.968Z
x_frame_options_missing	https://forums.fiservls.com/	https://forums.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.940Z
x_frame_options_missing	http://pop.fiservls.com/	http://pop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.920Z
x_frame_options_missing	https://corp.fiservls.com/	https://corp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.904Z
x_frame_options_missing	http://131.fiservls.com/	http://131.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.897Z
x_frame_options_missing	https://apps.fiservls.com/	https://apps.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.857Z
x_frame_options_missing	https://atlanta.fiservls.com/	https://atlanta.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.851Z
x_frame_options_missing	http://corp.fiservls.com/	http://corp.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.819Z
x_frame_options_missing	http://apps.fiservls.com/	http://apps.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.789Z
x_frame_options_missing	https://customer.fiservls.com/	https://customer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.784Z
x_frame_options_missing	https://intranet1.fiservls.com/	https://intranet1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.756Z
x_frame_options_missing	http://atlanta.fiservls.com/	http://atlanta.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.748Z
x_frame_options_missing	https://18.fiservls.com/	https://18.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.716Z
x_frame_options_missing	http://customer.fiservls.com/	http://customer.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.710Z
x_frame_options_missing	https://administrador.fiservls.com/	https://administrador.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.681Z
x_frame_options_missing	http://intranet1.fiservls.com/	http://intranet1.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.673Z
x_frame_options_missing	http://18.fiservls.com/	http://18.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.638Z
x_frame_options_missing	http://administrador.fiservls.com/	http://administrador.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.606Z
x_frame_options_missing	https://backup.fiservls.com/	https://backup.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.590Z
x_frame_options_missing	https://apollo.fiservls.com/	https://apollo.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.577Z
x_frame_options_missing	https://manage.fiservls.com/	https://manage.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.496Z
x_frame_options_mis	http://apollo.fiservls.c	http://apollo.fiservls.co	n/a	Header missing	2019-01-

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

sing	om/	m/			22T07:04:02.487Z
x_frame_options_missing	https://support.fiservls.com/	https://support.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.457Z
x_frame_options_missing	http://manage.fiservls.com/	http://manage.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.415Z
x_frame_options_missing	http://support.fiservls.com/	http://support.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.382Z
x_frame_options_missing	http://au.fiservls.com/	http://au.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.382Z
x_frame_options_missing	https://email.fiservls.com/	https://email.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.113Z
x_frame_options_missing	https://ad.fiservls.com/	https://ad.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.039Z
x_frame_options_missing	http://email.fiservls.com/	http://email.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.030Z
x_frame_options_missing	https://download.fiservls.com/	https://download.fiservls.com/	n/a	Header missing	2019-01-22T07:04:02.000Z
x_frame_options_missing	http://ad.fiservls.com/	http://ad.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.957Z
x_frame_options_missing	https://am.fiservls.com/	https://am.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.913Z
x_frame_options_missing	http://am.fiservls.com/	http://am.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.824Z
x_frame_options_missing	https://california.fiservls.com/	https://california.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.632Z
x_frame_options_missing	https://antivirus.fiservls.com/	https://antivirus.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.624Z
x_frame_options_missing	https://ajax.fiservls.com/	https://ajax.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.621Z
x_frame_options_missing	https://pop.fiservls.com/	https://pop.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.617Z
x_frame_options_missing	https://mail.fiservls.com/	https://mail.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.617Z
x_frame_options_missing	http://ajax.fiservls.com/	http://ajax.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z
x_frame_options_missing	http://antivirus.fiservls.com/	http://antivirus.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z
x_frame_options_missing	http://california.fiservls.com/	http://california.fiservls.com/	n/a	Header missing	2019-01-22T07:04:01.560Z

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

RECOMMENDATION

Add one of the following headers, using the 'DENY' or 'ALLOW-FROM' directive, to responses from this website: X-Frame-Options: DENY' X-Frame-Options: ALLOW-FROM https://example.com/'

ABOUT THIS ISSUE

The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a '<frame>', '<iframe>' or '<object>'. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other websites.

APPLICATION SECURITY > ISSUE DETAIL

! Session Cookie Missing 'HttpOnly' Attribute

Data may be exposed to unauthorized parties during cookie transmission and increases the risk of cross-site scripting (XSS) attacks.

-0.2 SCORE IMPACT

2 findings

HOSTNAME	URL	COOKIE NAME	RAW COOKIE	LAST SEEN
www.fiserv-ecomhosting.com	http://fiserv-ecomhosting.com/	ASPSESSIONID	ASPSESSIONIDCWTATADB=JPGJJLAAMKBDFLCBBPGBDHNM; secure; path=/	2019-01-30T00:00:00.000Z
fiserv-ecomhosting.com	https://fiserv-ecomhosting.com/	ASPSESSIONID	ASPSESSIONIDCWTATADB=LPGJJLAALLENJEIODEAFGJIN; secure; path=/	2019-01-30T00:00:00.000Z

RECOMMENDATION

Set session cookies with the 'HttpOnly' attribute to ensure they can not be accessed by any other means. A cookie marked with 'HttpOnly' will prevent any malicious injected scripts from being able to access it.

ABOUT THIS ISSUE

The cookie session ID is not set with the 'HttpOnly' attribute. The missing attribute could allow the session ID to be accessed by a client side script such as JavaScript. This exposes the cookies to potential theft via scripting attack vectors, such as XSS attacks.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

C 70 CUBIT SCORE

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

This proprietary module measures a variety of security issues that a company might have. For example, we check public threat intelligence databases for IP addresses that have been flagged. These misconfigurations may have high exploitability and could cause significant harm to the privacy of your data and infrastructure.

!!! HIGH SEVERITY

There are no High Risk Issues to detect for Cubit Score

!! MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Cubit Score

! LOW SEVERITY

Exposed Subdomain	3

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Cubit Score

i INFORMATIONAL

Possible Typosquat Domains Detected	0

CUBIT SCORE > ISSUE DETAIL

! Exposed Subdomain

An administrative subdomain was detected on public Internet. That subdomain may be vulnerable to unauthorized access.

-1.0 SCORE IMPACT

3 findings

SUBDOMAIN
admin.fiservcreditservices.com
intranet.fiserv.com
intranet.fiservpit.com

RECOMMENDATION

Resolve all private subdomains using a segregated, internal DNS server. If public exposure is required for these subdomains, it is advised that the integration prevent unauthorized access to the subdomains, either through exploitation or credential compromise. Implementing an IP whitelist for access to internal administrative subdomains would restrict unauthorized access attempts from successfully connecting via the public Internet.

ABOUT THIS ISSUE

A subdomain was detected on target domain names that are accessible to the public Internet. There is a possibility that this subdomain may be a portal to administrative functionalities for various enterprise applications.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

A 100 HACKER CHATTER

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The SecurityScorecard Hacker Chatter module is an automated collection and aggregation system for the analysis of multiple streams of underground hacker chatter. Forums, IRC, social networks, and other public repositories of hacker community discussions are continuously monitored, collected and aggregated in order to locate mentions of business names and websites. The Hacker Chatter score is an informational indicator ranking that is ranked based on the quantity of indicators that appear within the collection sensors.

!!! HIGH SEVERITY

There are no High Risk Issues to detect for Hacker Chatter

!! MEDIUM SEVERITY

Booter Shells Identified	0
Defacement	0

! LOW SEVERITY

There are no Low Risk Issues to detect for Hacker Chatter

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Hacker Chatter

i INFORMATIONAL

Hacker Chatter Mention	0

No issues found.

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

A 100 INFORMATION LEAK

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

This Information Leak module makes use of chatter monitoring and deep web monitoring capabilities to identify compromised credentials being circulated by hackers. These come in the form of bulk data breaches announced publicly as well as smaller breaches, and smaller exchanges between hackers.

!!! HIGH SEVERITY

There are no High Risk Issues to detect for Information Leak

!! MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Information Leak

! LOW SEVERITY

Sensitive Application Information Exposed (GitHub)	0
Sensitive Application Information Exposed (Google)	0
Credentials at Risk	0

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Information Leak

i INFORMATIONAL

There are no Info Risk Issues to detect for Information Leak

No issues found.

A 100 SOCIAL ENGINEERING

ISSUE COUNT

The table below includes a list of issues searched for and indicates which issues were found.

ABOUT THIS FACTOR

The SecurityScorecard Social Engineering Module is used to determine the potential susceptibility of an organization to a targeted social engineering attack. The Social Engineering module ingests data from social networks and public data breaches, and blends proprietary analysis methods. The Social Engineering Score is an informational indicator calculated based on the quantity of indicators that appear in SecurityScorecard collection sensors.

!!! HIGH SEVERITY

There are no High Risk Issues to detect for Social Engineering

!! MEDIUM SEVERITY

There are no Medium Risk Issues to detect for Social Engineering

! LOW SEVERITY

Employee Satisfaction	0
Corporate Email Used on Marketing Sites	0
Corporate Email Used on Short-Term Lending Sites	0

✓ POSITIVE SIGNALS

There are no Positive Risk Issues to detect for Social Engineering

i INFORMATIONAL

Leaked Company Emails Open to Spear-Phishing	62

Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

No content (including ratings, data, reports, software or other application or output therefrom) or any part thereof (collectively, Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system without the prior written permission of SecurityScorecard, Inc. (SSC) The Content shall not be used for any unlawful or unauthorized purposes.

SSC and any third-parties, and their directors, officers, shareholders, employees, customers and agents (collectively SSC Parties) do not guarantee or warrant the accuracy, completeness, timeliness or availability of the Content. SSC Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of the Content. The Content is provided on an "as is" basis. SSC PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS,(3) FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall SSC Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

USERS OF THE CONTENT MUST USE ALL REASONABLE ENDEAVORS TO MITIGATE ANY LOSS OR DAMAGE WHATSOEVER (AND HOWSOEVER ARISING) AND NOTHING HEREIN SHALL BE DEEMED TO RELIEVE OR ABROGATE USERS OF ANY SUCH DUTY TO MITIGATE ANY LOSS OR DAMAGE.

IN ANY EVENT, TO THE EXTENT PERMITTED BY LAW, THE AGGREGATE LIABILITY OF THE SSC PARTIES FOR ANY REASON WHATSOEVER RELATED TO ACCESS TO OR USE OF CONTENT SHALL NOT EXCEED THE GREATER OF (A) THE TOTAL AMOUNT PAID TO SSC BY THE USER FOR SERVICES PROVIDED DURING THE 12 MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY, AND (B) U.S. $100.

Security-related analyses, including ratings and statements in the Content, are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SSC's opinions, analyses and ratings should not be relied on as a substitute for the skill, judgment and experience of the user and its management, employees, advisors andr clients when making business decisions. SSC assumes no obligation to update the Content following publication in any form or format. While SSC has obtained information from sources it believes to be reliable, SSC does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives. Users expressly agree that (a) the security ratings and other security opinions provided via the Content do not reflect, identify or detect every vulnerability or security issue or address any other risk; (b) the security ratings and other opinions provided do not take into account users' particular objectives, situations or needs; (c) each rating or other opinion will be weighed, if at all, solely as one factor in any decision made by or on behalf of any user; and (d) users will accordingly, with due care, make their own study and evaluation of the risks of doing business with any entity. If a user identifies any in the Content, we invite you to share that information with us by emailing us at support@securityscorecard.io.